DOVER DISTRICT COUNCIL

Democratic Services
White Cliffs Business Park
Dover
Kent CT16 3PJ

Telephone: (01304) 821199
Fax: (01304) 872452
DX: 6312
Minicom: (01304) 820115
Website: www.dover.gov.uk
e-mail: democraticservices@dover.gov.uk

22 December 2016

Dear Councillor

NOTICE IS HEREBY GIVEN THAT a meeting of the **CABINET** will be held at these offices (Council Chamber) on Monday 9 January 2017 at 11.00 am when the following business will be transacted.

Members of the public who require further information are asked to contact Kate Batty-Smith on (01304) 872303 or by e-mail at kate.batty-smith@dover.gov.uk.

Yours sincerely

Chief Executive

Cabinet Membership:

P A Watkins	Leader of the Council
M D Conolly	Deputy Leader of the Council
T J Bartlett	Portfolio Holder for Property Management and Public Protection
P M Beresford	Portfolio Holder for Housing, Health and Wellbeing
N J Collor	Portfolio Holder for Access and Licensing
N S Kenton	Portfolio Holder for Environment, Waste and Planning
K E Morris	Portfolio Holder for Skills, Training, Tourism, Voluntary Services and Community Safety

AGENDA

1 **APOLOGIES**

To receive any apologies for absence.

2 **DECLARATIONS OF INTEREST** (Page 5)

To receive any declarations of interest from Members in respect of business to be transacted on the agenda.

3 **RECORD OF DECISIONS** (Pages 6-20)

The Decisions of the meetings of the Cabinet held on 5 and 15 December 2016 numbered CAB 94 to CAB 112 (inclusive) are attached.

4 **NOTICE OF FORTHCOMING KEY DECISIONS** (Pages 21-23)

The Notice of Forthcoming Key Decisions is included in the agenda to enable the Cabinet to identify future agenda items of public interest that should be subject to pre-scrutiny.

ISSUES ARISING FROM OVERVIEW AND SCRUTINY OR OTHER COMMITTEES

To consider any issues arising from Overview and Scrutiny or other Committees not specifically detailed elsewhere on the agenda.

5 **DOVER LEISURE CENTRE - SPA FEASIBILITY STUDY**

To consider the recommendations of the Scrutiny (Policy and Performance) Committee (to follow).

6 **DOVER LEISURE CENTRE - BUILDING CONTRACTOR PROCUREMENT**

To consider the recommendations of the Scrutiny (Policy and Performance) Committee (to follow).

7 **RECYCLING REWARD SCHEME**

To consider the recommendations of the Scrutiny (Policy and Performance) Committee (to follow).

8 **DRAFT WATERLOO CRESCENT CONSERVATION AREA CHARACTER APPRAISAL**

To consider the recommendations of the Scrutiny (Policy and Performance) Committee (to follow).

9 **PROVISION OF ACCESS EQUIPMENT AND SERVICES FOR NEW WINDOWS AND EXTERNAL DECORATION AT CANADIAN ESTATE, DOVER**

To consider the recommendations of the Scrutiny (Policy and Performance) Committee (to follow).

10 **ENFORCEMENT AND MONITORING OF PLANNING CONDITIONS**

To consider the recommendations of the Scrutiny (Community and Regeneration) Committee (to follow).

EXECUTIVE - KEY DECISIONS

11 **ADOPTION OF NELSON STREET, DEAL CONSERVATION AREA CHARACTER APPRAISAL** (Pages 24-47)

To consider the attached report of the Chief Executive.

Responsibility: Portfolio Holder for Environment, Waste and Planning

12 **FEES AND CHARGES 2017/18** (Pages 48-112)

To consider the attached report of the Director of Finance, Housing and Community

Responsibility: Portfolio Holder for Corporate Resources and Performance

EXECUTIVE - NON-KEY DECISIONS

13 **INFORMATION SECURITY, RISK AND GOVERNANCE FRAMEWORK AND POLICIES** (Pages 113-267)

To consider the attached report of the Director of Governance.

Responsibility: Portfolio Holder for Corporate Resources and Performance

14 **GUIDANCE ON SUSPECT DEVICES, PACKAGES AND CALLS** (Pages 268-278)

To consider the attached report of the Director of Governance.

Responsibility: Portfolio Holder for Corporate Resources and Performance

15 **EXCLUSION OF THE PRESS AND PUBLIC** (Page 279)

The recommendation is attached.

MATTERS WHICH THE MANAGEMENT TEAM SUGGESTS SHOULD BE CONSIDERED IN PRIVATE AS THE REPORT CONTAINS EXEMPT INFORMATION AS DEFINED WITHIN PART 1 OF SCHEDULE 12A OF THE LOCAL GOVERNMENT ACT 1972 AS INDICATED AND IN RESPECT OF WHICH THE PROPER OFFICER CONSIDERS THAT THE PUBLIC INTEREST IN MAINTAINING THE EXEMPTION OUTWEIGHS THE PUBLIC INTEREST IN DISCLOSING THE INFORMATION

EXECUTIVE - NON-KEY DECISIONS

16 **COMPENSATION PAYMENT** (Pages 280-281)

To consider the attached report of the Director of Environment and Corporate Assets.

Responsibility: Portfolio Holder for Property Management and Public Protection

Access to Meetings and Information

- Members of the public are welcome to attend meetings of the Council, its Committees and Sub-Committees. You may remain present throughout them except during the consideration of exempt or confidential information.

- All meetings are held at the Council Offices, Whitfield unless otherwise indicated on the front page of the agenda. There is disabled access via the Council Chamber entrance and a disabled toilet is available in the foyer. In addition, there is a PA system and hearing loop within the Council Chamber.

- Agenda papers are published five clear working days before the meeting. Alternatively, a limited supply of agendas will be available at the meeting, free of charge, and all agendas, reports and minutes can be viewed and downloaded from our website www.dover.gov.uk. Minutes will be published on our website as soon as practicably possible after each meeting. All agenda papers and minutes are available for public inspection for a period of six years from the date of the meeting.

- If you require any further information about the contents of this agenda or your right to gain access to information held by the Council please contact Kate Batty-Smith, Democratic Support Officer, telephone: (01304) 872303 or email: kate.batty-smith@dover.gov.uk for details.

Large print copies of this agenda can be supplied on request.

Declarations of Interest

Disclosable Pecuniary Interest (DPI)

Where a Member has a new or registered DPI in a matter under consideration they must disclose that they have an interest and, unless the Monitoring Officer has agreed in advance that the DPI is a 'Sensitive Interest', explain the nature of that interest at the meeting. The Member must withdraw from the meeting at the commencement of the consideration of any matter in which they have declared a DPI and must not participate in any discussion of, or vote taken on, the matter unless they have been granted a dispensation permitting them to do so. If during the consideration of any item a Member becomes aware that they have a DPI in the matter they should declare the interest immediately and, subject to any dispensations, withdraw from the meeting.

Other Significant Interest (OSI)

Where a Member is declaring an OSI they must also disclose the interest and explain the nature of the interest at the meeting. The Member must withdraw from the meeting at the commencement of the consideration of any matter in which they have declared a OSI and must not participate in any discussion of, or vote taken on, the matter unless they have been granted a dispensation to do so or the meeting is one at which members of the public are permitted to speak for the purpose of making representations, answering questions or giving evidence relating to the matter. In the latter case, the Member may only participate on the same basis as a member of the public and cannot participate in any discussion of, or vote taken on, the matter and must withdraw from the meeting in accordance with the Council's procedure rules.

Voluntary Announcement of Other Interests (VAOI)

Where a Member does not have either a DPI or OSI but is of the opinion that for transparency reasons alone s/he should make an announcement in respect of a matter under consideration, they can make a VAOI. A Member declaring a VAOI may still remain at the meeting and vote on the matter under consideration.

Note to the Code:

Situations in which a Member may wish to make a VAOI include membership of outside bodies that have made representations on agenda items; where a Member knows a person involved, but does not have a close association with that person; or where an item would affect the well-being of a Member, relative, close associate, employer, etc. but not his/her financial position. It should be emphasised that an effect on the financial position of a Member, relative, close associate, employer, etc OR an application made by a Member, relative, close associate, employer, etc would both probably constitute either an OSI or in some cases a DPI.

Record of the decisions of the meeting of the **CABINET** held at the Council Offices, Whitfield on Monday, 5 December 2016 at 11.00 am.

Present:

Chairman:	Councillor M D Conolly
Councillors:	T J Bartlett P M Beresford N J Collor N S Kenton K E Morris
Also Present:	Councillor S F Bannister Councillor S S Chandler Councillor M R Eddy Councillor P Walker
Officers:	Chief Executive Director of Environment and Corporate Assets Director of Finance, Housing and Community Director of Governance Director of Property Services (East Kent Housing) Head of Strategic Housing Policy and Projects Manager Waste Services Manager PR and Marketing Officer Senior Heritage Officer Democratic Support Officer

The formal decisions of the executive are detailed in the following schedule.

Record of Decisions: Executive Functions

Decision Status	Record of Decision	Alternative options considered and rejected (if any)	Reasons for Decision	Conflicts of interest (if any) declared by decision maker(s) or consultees (if any)
CAB 94 5.12.16 Open **Key Decisions** No **Call-in to apply** Yes **Implementation Date** 13 December 2016	APOLOGIES It was noted that Councillor P A Watkins had sent an apology for absence.	None.	To note any apologies for absence.	

Decision Status	Record of Decision	Alternative options considered and rejected (if any)	Reasons for Decision	Conflicts of interest (if any) declared by decision maker(s) or consultees (if any)
CAB 95 5.12.16 Open **Key Decisions** No **Call-in to apply** Yes	DECLARATIONS OF INTEREST It was noted that there were no declarations of interest.	None.	To note any declarations of interest.	

Implementation Date 13 December 2016				

Decision Status	Record of Decision	Alternative options considered and rejected (if any)	Reasons for Decision	Conflicts of interest (if any) declared by decision maker(s) or consultees (if any)
CAB 96 5.12.16 **Key Decisions** No **Call-in to apply** Yes **Implementation Date** 13 December 2016	RECORD OF DECISIONS It was agreed that the decisions of the meetings of the Cabinet held on 7, 21 and 28 November 2016, as detailed in decision numbers CAB 67 to CAB 93, be approved as correct records and signed by the Chairman.	None.	Cabinet is required to approve the Records of Decisions of the Cabinet meetings held on 7, 21 and 28 November 2016.	

Decision Status	Record of Decision	Alternative options considered and rejected (if any)	Reasons for Decision	Conflicts of interest (if any) declared by decision maker(s) or consultees (if any)
CAB 97 5.12.16 Open **Key Decisions** No **Call-in to apply** Yes	NOTICE OF FORTHCOMING KEY DECISIONS It was agreed that there were no forthcoming Key Decisions identified for pre-Scrutiny at this stage.	None.	Cabinet is requested to identify any Key Decisions that it considers would be beneficial to refer to one of the Scrutiny Committees before	

Implementation Date 13 December 2016			the matter comes before Cabinet for formal decision.	

Decision Status	Record of Decision	Alternative options considered and rejected (if any)	Reasons for Decision	Conflicts of interest (if any) declared by decision maker(s) or consultees (if any)
CAB 98 5.12.16 Open **Key Decisions** No **Call-in to apply** Yes **Implementation Date** 13 December 2016	<u>LORRY PARKING SURVEY UPDATE</u> It was agreed: (a) That the Scrutiny (Policy and Performance) Committee's recommendation (a), made at its meeting held on 15 November 2016 (Minute No 87, be approved, subject to the caveat that the 11.00pm to 4.00am period be included in the next enforcement survey as a one-off check only. (b) That the Scrutiny (Policy and Performance) Committee's recommendations (b) (i) to (iii) be approved, subject to Kent County Council, as the Highways Authority, also being lobbied in respect of the Traffic Management Act and the payment of parking fines by foreign-registered vehicles.	To approve the recommendations without amendment.	At its request, the Scrutiny (Policy and Performance) Committee, at its meeting held on 15 November 2016, received an update on lorry parking issues in the District and made recommendations to Cabinet.	

Decision Status	Record of Decision	Alternative options considered and rejected (if any)	Reasons for Decision	Conflicts of interest (if any) declared by decision maker(s) or consultees (if any)
CAB 99 5.12.16 Open	<u>ENVIRONMENTAL ENFORCEMENT SERVICE DELIVERY OPTIONS</u> It was agreed:	None.	The Scrutiny (Policy and Performance)	

Key Decisions Yes **Call-in to apply** Yes **Implementation Date** 13 September 2016	(a) That the Scrutiny (Policy and Performance) Committee's endorsement of Cabinet decision CAB 75, made at its meeting held on 7 November 2016 (Minute No 89), be acknowledged. (b) That Cabinet decision CAB 75 be reaffirmed.		Committee, at its meeting held on 15 November 2016, endorsed Cabinet decision CAB 75 of 7 November 2016.	

Decision Status	Record of Decision	Alternative options considered and rejected (if any)	Reasons for Decision	Conflicts of interest (if any) declared by decision maker(s) or consultees (if any)
CAB 100 5.12.16 Open **Key Decisions** Yes **Call-in to apply** Yes **Implementation Date** 13 December 2016	<u>INTRODUCTION OF FIXED PENALTY NOTICES FOR FLY-TIPPING</u> It was agreed: (a) That the Scrutiny (Policy and Performance) Committee's endorsement of Cabinet decision CAB 76, made at its meeting held on 15 November 2016 (Minute No 90), be acknowledged. (b) That Cabinet decision CAB 76 be reaffirmed.	None.	The Scrutiny (Policy and Performance) Committee, at its meeting held on 15 November 2016, endorsed Cabinet decision CAB 76 of 7 November 2016.	

Decision Status	Record of Decision	Alternative options considered and rejected (if any)	Reasons for Decision	Conflicts of interest (if any) declared by decision maker(s) or consultees (if any)
CAB 101	<u>PERFORMANCE REPORT - SECOND QUARTER 2016/17</u>	None.	The Scrutiny	

5.12.16 Open **Key Decisions** No **Call-in to apply** Yes **Implementation Date** 13 December 2016	It was agreed: (a) That the Scrutiny (Policy and Performance) Committee's endorsement of Cabinet decision CAB 78, made at its meeting held on 15 November 2016 (Minute No 91), be acknowledged. (b) That Cabinet decision CAB 78 be reaffirmed.		(Policy and Performance) Committee, at its meeting held on 15 November 2016, endorsed Cabinet decision CAB 78 of 7 November 2016.	

Decision Status	Record of Decision	Alternative options considered and rejected (if any)	Reasons for Decision	Conflicts of interest (if any) declared by decision maker(s) or consultees (if any)
CAB 102 5.12.16 Open **Key Decisions** Yes **Call-in to apply** Yes **Implementation Date** 13 December 2016	<u>AWARD OF CONTRACT FOR GAS SERVICING AND HEATING INSTALLATIONS</u> It was agreed: (a) That the Scrutiny (Policy and Performance) Committee's endorsement of Cabinet decision CAB 81, made at its meeting held on 15 November 2016 (Minute No 93), be acknowledged. (b) That Cabinet decision CAB 81 be reaffirmed.	None.	The Scrutiny (Policy and Performance) Committee, at its meeting held on 15 November 2016, endorsed Cabinet decision CAB 81 of 7 November 2016.	

Decision Status	Record of Decision	Alternative options considered and rejected (if any)	Reasons for Decision	Conflicts of interest (if any) declared by decision maker(s) or

				consultees (if any)
CAB 103 5.12.16 Open **Key Decisions** Yes **Call-in to apply** Yes **Implementation Date** 13 December 2016	AYLESHAM VILLAGE EXPANSION - UPDATE AND DEED OF VARIATION It was agreed: (a) That the Scrutiny (Community and Regeneration) Committee's endorsement of Cabinet decision CAB 80, made at its meeting held on 16 November 2016 (Minute No 58), be acknowledged. (b) That the Scrutiny (Community and Regeneration) Committee's recommendation (b) be rejected since it is for Cabinet to prioritise where capital receipts should be allocated across the whole District. (c) That Cabinet decision CAB 80 be reaffirmed.	To accept Scrutiny's additional recommendation.	The Scrutiny (Community and Regeneration) Committee, at its meeting held on 16 November 2016, endorsed Cabinet decision CAB 80 of 7 November 2016 and made an additional recommendation.	

Decision Status	Record of Decision	Alternative options considered and rejected (if any)	Reasons for Decision	Conflicts of interest (if any) declared by decision maker(s) or consultees (if any)
CAB 104 5.12.16 Open **Key Decisions** Yes **Call-in to apply** Yes **Implementation Date** 13 December	RECYCLING REWARD SCHEME It was agreed: (a) That the implementation of a recycling reward scheme, to be funded from funding awarded to the Council by the Department for Communities and Local Government, be approved. (b) That the Director of Environment and Corporate Assets be authorised to procure a provider to administer and host the scheme. (c) That a report be brought back to Cabinet in February/March 2017	To not amend the report recom-mendations.	Following a joint application, Dover and Shepway District Councils have received funding of £720,486 from the Department for Communities and Local Government to implement a recycling reward scheme across	

2016	with further details of the proposed scheme.		both districts.	

Decision Status	Record of Decision	Alternative options considered and rejected (if any)	Reasons for Decision	Conflicts of interest (if any) declared by decision maker(s) or consultees (if any)
CAB 105 5.12.16 Open **Key Decisions** No **Call-in to apply** Yes **Implementation Date** 13 December 2016	<u>DRAFT WATERLOO CRESCENT, DOVER CONSERVATION AREA APPRAISAL</u> It was agreed: (a) That the draft Waterloo Crescent Conservation Area Character Appraisal, set out at Appendix 1 of the report, be approved for a period of 6 weeks' public consultation. (b) That the Head of Regeneration and Development be authorised, in consultation with the Portfolio Holder for Environment, Waste and Planning, to make any necessary editorial changes to the appraisal prior to consultation in order to assist with clarity, consistency, explanation and presentation.	None.	Under the Planning (Listed Buildings and Conservation Areas) Act 1990, there is a requirement for local authorities to review their conservation areas and to publish proposals for their preservation and enhancement. The draft Waterloo Crescent Conservation Area Character Appraisal supports one of the key recommendations in the Dover District Heritage Strategy and will be used to help inform the emerging plans for the Dover Waterfront	

			Masterplan.	

Decision Status	Record of Decision	Alternative options considered and rejected (if any)	Reasons for Decision	Conflicts of interest (if any) declared by decision maker(s) or consultees (if any)
CAB 106 5.12.16 Open **Key Decisions** No **Call-in to apply** Yes **Implementation Date** Immediate	EXCLUSION OF THE PRESS AND PUBLIC That, in accordance with the provision of the Local Authorities (Executive Arrangements) (Access to Information) (England) Regulations 2000, the press and the public be excluded during consideration of the following item of business on the grounds that it involves the likely disclosure of exempt information as defined in paragraph 3 of Schedule 12A of the Local Government Act 1972.	None.		

Decision Status	Record of Decision	Alternative options considered and rejected (if any)	Reasons for Decision	Conflicts of interest (if any) declared by decision maker(s) or consultees (if any)
CAB 107 5.12.16 Exempt **Key Decisions** Yes **Call-in to apply** Yes **Implementation**	PROVISION OF ACCESS EQUIPMENT AND SERVICES FOR NEW WINDOWS AND EXTERNAL DECORATION AT CANADIAN ESTATE, DOVER It was agreed that the contract between Anglian Building Products Ltd and Dover District Council be increased by the sum set out in paragraph 3 of the report to allow for progression of the recommended option, including the cost of access. The contract will be revised to the sum set out in paragraph 6 of the report.	None.	The current contract between Dover District Council and Anglian Building Products Ltd to install new windows (and carry out external repairs and decoration) at the Canadian	

Date 13 December 2016			Estate makes no provision for access arrangements (e.g. scaffolding, etc) and must therefore be varied to cover this additional cost.	

The meeting ended at 11.38 am

Record of the decisions of the special meeting of the **CABINET** held at the Council Offices, Whitfield on Thursday, 15 December 2016 at 10.00 am.

Present:

Chairman:	Councillor M D Conolly
Councillors:	T J Bartlett P M Beresford N J Collor N S Kenton
Also Present:	Councillor S F Bannister Councillor P M Brivio Councillor M R Eddy Councillor B Gardner Councillor P Walker
Officers:	Chief Executive Director of Environment and Corporate Assets Director of Finance, Housing and Community Director of Governance Head of Finance Procurement Manager Principal Infrastructure and Delivery Officer Principal Leisure Officer Democratic Support Officer

The formal decisions of the executive are detailed in the following schedule.

Record of Decisions: Executive Functions

Decision Status	Record of Decision	Alternative options considered and rejected (if any)	Reasons for Decision	Conflicts of interest (if any) declared by decision maker(s) or consultees (if any)
CAB 108 15.12.16 Open **Key Decisions** No **Call-in to apply** Yes **Implementation Date** 23 December 2016	<u>APOLOGIES</u> It was noted that Councillors K E Morris and P A Watkins had sent apologies for absence.	None.		

Decision Status	Record of Decision	Alternative options considered and rejected (if any)	Reasons for Decision	Conflicts of interest (if any) declared by decision maker(s) or consultees (if any)
CAB 109 15.12.16 Open **Key Decisions** No **Call-in to apply** Yes	<u>DECLARATIONS OF INTEREST</u> It was noted that there were no declarations of interest.	None.		

Implementation Date 23 December 2016				

Decision Status	Record of Decision	Alternative options considered and rejected (if any)	Reasons for Decision	Conflicts of interest (if any) declared by decision maker(s) or consultees (if any)
CAB 110 15.12.16 Open **Key Decisions** No **Call-in to apply** Yes **Implementation Date** 23 December 2016	EXCLUSION OF THE PRESS AND PUBLIC That, in accordance with the provisions of the Local Authorities (Executive Arrangements) (Access to Information) (England) Regulations 2000, the press and the public be excluded during consideration of the following items of business on the grounds that they involve the likely disclosure of exempt information as defined in paragraph 3 of Schedule 12A of the Local Government Act 1972.	None.		

Decision Status	Record of Decision	Alternative options considered and rejected (if any)	Reasons for Decision	Conflicts of interest (if any) declared by decision maker(s) or consultees (if any)
CAB 111 15.12.16 Exempt **Key Decisions** Yes **Call-in to apply**	DOVER LEISURE CENTRE - SPA FEASIBILITY STUDY It was agreed: (a) That the Dover Leisure Centre Project Advisory Group's recommendation, made at its meeting held on 8 December 2016 (Minute No 62), be approved as follows:	None.	At its meeting held on 20 September 2016, Cabinet agreed the site of, and facility mix for, a new leisure centre and commissioned a	

Yes **Implementation Date** 23 December 2016	'That the Council should not proceed with the spa facility, and the project should proceed as planned but with an increased services capacity (at a cost of £39,000 plus VAT).' (b) That the facility mix of the new Leisure Centre, as approved by Cabinet at its meeting held on 20 September 2016 (CAB 50), be confirmed subject to the addition of increased services capacity (at a cost of £39,000) so that a spa or other additional facility can be added at a later date. (c) That the Director of Environment and Corporate Assets be authorised to: (i) Submit an application for planning consent for a new leisure centre at Whitfield, in consultation with the Portfolio Holder for Property Management and Public Protection. (ii) Determine any appropriate development contributions to be offered as part of the application, in consultation with the Portfolio Holder for Corporate Resources and Performance.		report on the feasibility of adding a spa facility (CAB 50). This report has now been completed and is presented to Cabinet. At its meeting held on 8 December 2016, the Dover Leisure Centre Project Advisory Group recommended that a spa should not be proceeded with but that increased services capacity should be added to allow a spa or other facility to be built at a later date.	

Decision Status	Record of Decision	Alternative options considered and rejected (if any)	Reasons for Decision	Conflicts of interest (if any) declared by decision maker(s) or consultees (if any)
CAB 112 15.12.16 Exempt **Key Decisions** Yes	DOVER LEISURE CENTRE - BUILDING CONTRACTOR PROCUREMENT It was agreed that the appointment of BAM as the preferred contractor for the pre-construction phase, as set out at Appendix A to the report, be approved.	None.	Following a competitive tender process conducted through the Southern Contractors'	

Call-in to apply Yes **Implementation Date** 23 December 2016			Framework, Cabinet is requested to agree the appointment of a contractor for Stage One (the pre-construction phase) of the project.	

The meeting ended at 10.26 am

Notice of Forthcoming Key Decisions

[This updated version of the Notice supersedes all other versions issued in previous months]

Publication Date: 2 December 2016

Notice of Forthcoming Key Decisions which will be made on behalf of the Council

Key Decisions 2016/17	Item	Date of meeting at which decision will be taken by Cabinet (unless specified otherwise)
1	Preparation of the Dover District Council Draft Community Infrastructure Levy Charging Schedule	3 December 2012 and dates to be confirmed
2	Neighbourhood Plans	June 2013 and ongoing (see entry)
3	Gypsy, Traveller and Travelling Showpeople Development Plan	Date to be confirmed
4	Dover Town Centre Regeneration: To consider progress on the Compulsory Purchase Order and any issues arising which may go beyond the scope of the resolutions incorporated in Minute CAB 87	8 September 2014/24 April 2015/7 March 2016 and ongoing
5	Approval of the award of a contract for the electrical re-wiring of Council-owned properties	Date to be confirmed
6	Revised Hackney Carriage and Private Hire Licensing Policy	1 February 2016 and 4 July 2016
7	To consider: a) the result of consultation on the extension of the Kingsdown Conservation Area boundary and b) the introduction of an Article 4 Direction	a) 29 February 2016 b) 5 September 2016
8	To seek approval for the implementation of the Indoor Sports Facility Strategy and support the work being undertaken to replace Dover Leisure Centre.	7 March and 4 July 2016
9	Approval of Housing Adaptations Policy	9 May 2016
10	To seek Cabinet approval for public consultation on draft Nelson Street, Deal Conservation Area Appraisal	5 September 2016 and 9 January 2017
11	Future provision of Grounds Maintenance Services	9 May 2016
12	Extension to fitness suite at Tides Leisure Centre, Deal	Project delayed pending appointment of new operator for Tides Leisure Centre
13	Parking Strategy Review	9 May and 5 September 2016
14	Approval of Fuel Poverty Strategy for Kent	5 September 2016
15	Review of Aylesham Village Expansion Development Agreement	7 November 2016
16	Approval to develop detailed plans for replacement of Dover Leisure Centre	25 July/20 September and 15 December 2016 (special Cabinet meetings) and ongoing
17	Project approval for the refurbishment of Norman Tailyour House	5 September 2016

Key Decisions 2016/17	Item	Date of meeting at which decision will be taken by Cabinet (unless specified otherwise)
18	To agree the Council's requirements for the submission of financial viability assessments	Date to be confirmed (Developer Contributions Executive Committee)
19	Authority Monitoring Report	6 or 20 February 2017 (to be confirmed)
20	Statutory Brownfield Register	6 March 2017 (to be confirmed)
21	Review of Tenancy Strategy and Tenancy Policy	February-April 2017
22	Approval of draft Waterloo Crescent, Dover Conservation Area Appraisal for public consultation	5 December 2016 and date to be confirmed
23	To seek approval for the introduction of fixed penalty notices and the level to be set for fly-tipping offences under Section 33 of the Environmental Protection Act 1990	7 November 2016
24	Approval for the continuation of 'Energy Deal', the Collective Energy Switching Scheme	7 November 2016
25	To implement a recycling reward scheme	5 December 2016
26	Council Tax Reduction Scheme	21 November 2016
27	To approve the cost and contractual arrangements with regard to access to Canadian Estate properties for installation of replacement uPVC windows and redecoration	5 December 2016
28	Agreement on levels of Fees and Charges for 2017/18	9 January 2017
29	Recommendation to Council of the draft 2017/18 Budget and Medium-Term Financial Plan 2017/18-2020/21 and approval by Cabinet of various delegations within the Budget	6 and 20 February 2017
30	Thanet District Council Preferred Options Local Plan	20 February or 6 March 2017
31	Canterbury City Council Local Plan (Proposed Main Modifications)	20 February or 6 March 2017
32	To approve the award of a contract for the preparation of a planning application and an application for Scheduled Monument Consent for a Commonwealth War Memorial at Western Heights, Dover	Date to be confirmed
33	Appropriation of Assets	9 January 2017

Note: (1) Key Decisions which are shaded have already been taken and do not appear in this updated version of the Notice of Forthcoming Key Decisions.

(2) The Council's Corporate Management Team reserves the right to vary the dates set for consultation deadline(s) and for the submission of reports to Cabinet and Council in respect of Key Decisions included within this version of the notice. Members of the public can find out whether any alterations have been made by looking at the Council's website (www.dover.gov.uk).

Subject:	**ADOPTION OF THE NELSON STREET, DEAL CONSERVATION AREA CHARACTER APPRAISAL**
Meeting and Date:	**Cabinet – 9 January 2017**
Report of:	**Nadeem Aziz, Chief Executive**
Portfolio Holder:	**Councillor Nick Kenton, Portfolio Holder for Environment, Waste and Planning**
Decision Type:	**Key Decision**
Classification:	**Unrestricted**
Purpose of the report:	To inform Cabinet of the results of the public consultation exercise, and the proposed modifications to the Nelson Street, Deal Conservation Area Appraisal and to adopt it as a material consideration for planning purposes. The report also seeks Cabinet approval to undertake public consultation to extend the existing Conservation Area boundary and introduce an Article 4 Direction following the recommendations of the Deal Society.
Recommendation:	Cabinet agrees to: 1. the proposed responses to the representations received and the resulting modifications to the Nelson Street, Deal Conservation Area Character Appraisal as set out in Appendix 1; 2. adopt the Nelson Street, Deal Conservation Area Character Appraisal as a material consideration for planning purposes as set out in Appendix 2; 3. undertake further work to extend the Conservation Area boundary and to introduce an Article 4 Direction in response to the recommendations in the Nelson Street, Deal Conservation Area Character Appraisal; and 4. authorise the Head of Regeneration and Development to make any necessary editorial changes to the Nelson Street, Deal Conservation Area Appraisal to assist with clarity, consistency, explanation and presentation in conjunction with the Portfolio Holder.

1. Summary

1.1 Cabinet approved the Draft Nelson Street, Deal Conservation Area Appraisal for public consultation in September 2016. Consultation has now been undertaken and, following the analysis of representations, minor modifications are now proposed.

1.2 There are three key recommendations in the Appraisal:

1) Three extensions to the existing Conservation Area boundary;

2) Making of a Tree Preservation Order; and

3) Introduction of an Article 4 Direction which would remove certain permitted development rights in the Conservation Area.

1.3 If the recommendations are agreed, the District Council will have to follow separate formal procedures to extend the existing boundary of the Conservation Area, make a Tree Preservation Order and introduce an Article 4 Direction. These will include further public consultation.

2. Introduction and Background

2.1 At Cabinet on the 5th September 2016 the draft Nelson Street, Deal Conservation Area Appraisal was approved for public consultation. It had been prepared by the Deal Society, in conjunction with the District Council, following recommendations in the Dover District Heritage Strategy.

2.2 The consultation period ran for six weeks from 7th October until 18th November 2016 and the District Council received 3 responses from 3 individuals or organisations. There were no objections to the Conservation Area Appraisal and the findings were generally supported which is a credit to the hard work that the Deal Society have put into preparing the Appraisal.

2.3 Further to comments received during the consultation additional text, indicated in **bold** in the Appraisal, has been inserted to make the document more robust and to assist with the interpretation of the Appraisal.

2.4 A full list of representations received, together with the proposed District Council responses and amendments are set out in Appendix 1.

Proposed extensions to the existing Nelson Street, Deal Conservation Area boundary

3. Nelson Street, Deal Conservation Area was originally designated in 1977 and extended in 1994. Local councils are required under the Planning (Listed Buildings and Conservation Areas) Act 1990 to review their conservation areas from time to time to ensure that the original designation was correct, and to formulate and publish proposals for further enhancement and preservation of their conservation areas. This Appraisal has, therefore, been produced in compliance with this requirement.

3.1 The Appraisal has recommended three extensions to the existing Conservation Area boundary, as follows:

1) To include Faber Villa, Robert Street as the building has significant architectural and historic merit such that it makes a positive contribution to the character and appearance of the Conservation Area.

2) To include the small grassed space on Clarence Place adjacent to Faber Villa as this strip of land enhances the setting of the Conservation Area.

3) To include the section of Princes Street up to the junction with Ark Lane, which is currently not in the Conservation Area. The age and style of the buildings are similar and there is no logical reason for their omission from the boundary.

3.2 The proposed extensions to the Conservation Area are illustrated on the map in Appendix 3.

Tree Preservation Order

3.3 The Appraisal recommended the consideration of applying a Tree Preservation Order to a monkey puzzle tree that is within the rear garden of Prospect Cottage, Water Street, and which is visible from Garden Alley. The tree dominates the intimate space in Garden Alley and as trees within the Conservation Area are very few, the monkey puzzle tree makes a positive contribution to the character of the Conservation Area and as such warrants protection.

Article 4 Direction

3.4 The Appraisal has also recommended the introduction of an Article 4 Direction. An Article 4 Direction would remove permitted development rights for single residential dwellings, which in this case would be the properties that are located within the Conservation Area. Works identified in the Article 4 Direction, would require planning permission before they could be undertaken.

3.5 The proposed extensions to the Conservation Area, introduction of a Tree Preservation Order and an Article 4 Direction will need to go through separate formal procedures. The results of this public consultation will be reported back to Cabinet.

4. Identification of Options

4.1 Option 1: That the amendments to the Nelson Street, Deal Conservation Area Appraisal are agreed and it is adopted as a material consideration for planning purposes: or

4.2 Option 2: That the amendments to the Nelson Street, Deal Conservation Area Appraisal are not agreed and it is not adopted as a material consideration for planning purposes.

5. Evaluation of Options

5.1 The Appraisal would be used to identify opportunities for environmental improvements, inform new development and to act as an evidence base for the evaluation of new proposals. It would also be used by Planning Inspectors in appeal situations and, as it has been through a public consultation greater weight can also be attributed to it. It also provides the initial evidence for the District Council to start a review of the existing Conservation Area boundary, the introduction of a Tree Preservation Order and an Article 4 Direction, which would provide greater protection to the special character of the Conservation Area.

5.2 The Appraisal has been produced in response to the recommendations in the Dover District Heritage Strategy and the accompanying Action Plan. It, therefore, implements part of the Heritage Strategy.

5.3 If the Appraisal was not adopted, then the benefits outlined above would not be realised and the special character of the Conservation Area could be at risk through inappropriate development. The first option is, therefore, recommended.

6. Resource Implications

6.1 The Appraisal would be made available on the District Council's website. Further internal resources would be required to undertake public consultation relating to the

proposed changes to the Conservation Area boundary, Tree Preservation Order and the introduction of an Article 4 Direction.

7. Corporate Implications

7.1 Comment from the Section 151 Officer: ‘‘Finance has been consulted and has nothing further to add (SB)”.

7.2 Comment from the Solicitor to the Council: “The Solicitor to the Council has been consulted in the preparation of this report and has no further comments to make”.

7.2.1 Comment from the Equalities Officer: “The report does not specifically highlight any equality implications, however in discharging their responsibilities members are required to comply with the public sector duty as set out in section 149 of the Equality Act 2010 http://www.legislation.gov.uk/ukpga/2010/15”.

7.3 Other Officers (as appropriate): None.

8 Appendices

Appendix 1 – Analysis of Representations and Suggested District Council Response

Appendix 2 – Nelson Street, Deal Conservation Area Appraisal September 2016

Appendix 3 – Proposed extensions to the Nelson Street, Deal Conservation Area

Background Papers

Cabinet Report 5th September 2016.

Contact Officer: Alison Cummings, Principal Heritage Officer, extension 2464

APPENDIX 1: ANALYSIS OF PUBLIC REPRESENTATION

Number	Person ID	Full Name	Company / Organisation	Your Comment - Please enter your full representation in the box below with any changes you feel necessary.	Council's Response	Recommendation
1	604182	Mr David Skinner		Most of the houses in Duke Street, Nelson Street, Robert Street, Water Street, Princes Street and Water Street have basements with metal grills or glass covers set in the pavements. Some in Water Street have steps leading down to the basement. None of these characteristics have been mention in the Appraisal. The Work Houses that were on the site of St Andrews Church are first mentioned in Para 4.1 and then only in a single paragraph. Should a little more detail have been provided. The existing wall behind St Andrew Church is part of the wall of the work house. Should this be protected ?	Agree that basements are a key feature in Water Street in particular and that the appraisal should be amended to highlight them to a greater extent, however the railings and steps down to basements noted on Water St are modern alterations and not historic. Agree that the workhouse is an important part of the previous use of the land and that reference to it should be included in the historical overview, particularly as the boundary wall to the west of St Andrew Church is an original boundary to the workhouse.	Add text to section 1.1, introduction to include reference to workhouse; Amend where appraisal notes three storey buildings to two and basement; Add sentence in section 2.4 to highlight basements in Water St; Add further detail in section 2.7, St Andrew's Church to include detail on site of workhouse and evidence of wall; Add sentence in section 4.1 Historical Development to include date of workhouse.
2	507408	Mr William Elliott	Friends of North Deal	Friends of North Deal wish to commend the work carried out by the Deal Society on this appraisal, and to recommend that their conclusions be adopted. It will provide a level playing-field, under the Article 4 Direction, for both sides of Deal High Street in our Conservation Area.	Comments noted and welcomed.	Noted, no change proposed
3	409239	Lorna Crow	Deal Town Council	Deal Town Council fully support the appraisal and its recommendations.	Support noted.	Noted, no change proposed

Appendix 2

Nelson Street, Deal Conservation Area Appraisal

Draft

September 2016

Contents

1. Introduction

   1.1. Background
   1.2. Planning Policy Context
   1.3. Community Involvement
   1.4. Summary of Significance

2. The Character Appraisal

   2.1. Overview
   2.2. Duke Street
   2.3. Nelson Street
   2.4. Water Street
   2.5. Princes Street
   2.6. Robert Street
   2.7. St Andrew's Church, St Andrew's Road, Union Road and West Street

3. Management Plan
   3.1. Vulnerabilities and Negative Features
   3.2. Recommendations
      3.2.1. Extensions of boundary
      3.2.2. Tree Preservation Order
      3.2.3. Heritage Assets of local importance
      3.2.4. Article 4 Direction

4. Appendices
   4.1. Historical development
   4.2. Map showing proposed boundary changes
   4.3. Planning controls
      4.3.1. Article 4(1) Direction
      4.3.2. Tree Preservation Order
   4.4. Acknowledgements and references
   4.5. Glossary

1. Introduction

1.1. Background

The Nelson Street Conservation Area lies to the north and west of Deal High Street. It consists of 5 streets plus St. Andrew's Church and its grounds and small sections of West Street, Union Road and St. Andrew's Road. The conservation area contains about 200 buildings, of which five are Grade II listed and it was designated on the 21st July 1977. This appraisal was carried out during 2015.

Originally the site of large market gardens established in the 18th century to respond to the growth of shipping in the Downs off Deal and the development of the Dockyard**, and the location of the Deal Workhouse**, the area developed in the first half of the 19th century. This was largely in response to population growth during the Napoleonic wars when it grew by nearly 50%. The original town centre stretching from Elizabeth Carter House in South Street to the Town Hall could no longer accommodate the burgeoning population with new needs for employment and housing.

An appraisal is intended to provide an understanding of the special interest of a conservation area and to set out options and recommendations to help ensure that any changes are informed by an understanding of the local character and distinctiveness of the conservation area. ~~When this appraisal is adopted by Dover District Council (DDC) it~~ **This appraisal is** ~~will become~~ a material consideration in the determination of applications for planning permission within and adjacent to the conservation area.

This appraisal looks at the following issues:

1. The origins and evolution of the area under consideration.
2. The current boundary of the area and any review that should be made of that.
3. The positive and negative factors that contribute to or detract from the current condition of the conservation area.
4. Any recommendations that will protect and enhance the conservation area. Any changes proposed must sustain and enhance the historic environment and its heritage.

1.2. Planning Policy Context

The Planning (Listed Building and Conservation Areas) Act 1990 sets out the statutory definition of a Conservation Area, which is "an area of special architectural or historic interest, the character and appearance of which it is desirable to preserve or enhance" (s.69(1)). Dover District currently has 57 designated Conservation Areas.

There is a requirement under the legislation to review Conservation Areas "from time to time" to ensure that the boundary captures all the area that is of special interest and to assist in developing plans for the management of change within the conservation area. This is further endorsed by the National Planning Policy Framework (2012) which urges the need to ensure that an area justifies the designation because of its special architectural or historic character or appearance.

The Dover District Heritage Strategy (2013) presents the districts Heritage Assets as Themes; Theme 13 dealing with conservation areas. The districts conservation areas are considered to be heritage assets of **outstanding significance**, and in addition to being attractive places to live and work, contribute to the economic wealth of the district by being a magnet for visitors. Seven Conservation Areas lie within the area that the Deal Society undertook to monitor - four of these lie in the Town of Deal and three lie within the Parish of Walmer.

A methodology was developed for the Heritage Strategy enabling a rapid desk-based assessment of the general condition of the districts conservation areas and was applied to 19 of the conservation areas. The results of this overview, using a “traffic-light “system to classify their condition, indicate that of the 57 conservation areas in the district 12 of these conservation areas were identified as ‘performing well’ and achieved a green light, six achieved an amber light, requiring some enhancement, and one area required considerable enhancement or potential “de-designation” as a conservation area, due to the substantial loss of its character of special interest.

Theme 13 prescribes methods and techniques by which an area’s condition may be measured, assessed and managed; Article 4(2) Direction is one method. An Article 4(2) Direction removes permitted development rights from residential properties to ensure that certain changes, such as the replacement of windows, is managed to ensure that the change is appropriate to the special character of the conservation area. Article 4 Directions have been applied so far to two of the 19 conservation areas, one of them being the Middle Street Conservation Area in Deal.

The Heritage Strategy also suggested the formulation of a system for the assessment of a conservation areas condition such as that developed and adopted by the Oxford City Council, endorsed by Historic England and used by the Oxford Preservation Trust. That system has been used in this character appraisal, further informed by best practice guidance within the Historic England Advice Note 1: Conservation Area Designation, Appraisal and Management (Feb 2016).

1.3. Community Involvement

This character appraisal has been prepared by The Deal Society in close liaison with DDC. The Dover District Heritage Strategy highlights the importance of local community involvement in the protection of the historic environment. There are two specific areas where that involvement is encouraged. First of all, local civic groups are encouraged to develop appraisals of conservation areas within their locality. Secondly, the production of a List of Heritage Assets is encouraged. This appraisal is, therefore, consistent with the aspirations of the Heritage Strategy. (For a more detailed analysis of the Strategy see 1.2).

Every resident in this conservation area was informed by letter that the appraisal would be carried out during the summer of 2015. The letter also contained a short questionnaire to which the residents were invited to respond. The local parish magazine and The Deal Society newsletter also had ~~short~~ articles describing the purpose of the appraisal. One third of the residents responded to the questionnaire and the matters raised by them are reflected in the content of this **appraisal** ~~report~~.

~~The first draft of this appraisal was submitted to DDC in November 2015 in order for a process of public consultation to be agreed.~~

1.4. Summary of Significance

a. The historical development of the conservation area in the first half of the 19th century offers a major clue to its significance. Originally a large group of market gardens, the land was sold off in small plots to meet a housing crisis in the town as the nation engaged in the Napoleonic wars. A large influx of newcomers to meet the demands of the ships offshore created an urgent need for houses and rooms to buy and let. The response to that crisis was immediately seen in the creation of the streets of the conservation area.

b. The comparatively short historical development gives the area a strong sense of cohesion and continuity. It has remained relatively unchanged since the middle of the 19th century. There are a few 20th century additions especially in Robert Street but they do not fundamentally affect the overall character of the area.

c. There is some historical evidence, following the Pavement Act of 1791, that the layout of the streets on a loose grid pattern was a very early example of “town planning”. It was a very informal process and the evolution of most of the streets suggests different builders creating small terraces that evolved into the layout seen now.

d. Most of the streets consist of small terraces and individual houses built to the pavement. This creates a fairly narrow topography. The exception to this is the area around St. Andrew’s Church where the large formal space of the churchyard and gardens gives an almost rural feel. That is accentuated by the reinstated railings to the eastern edge of the gardens.

e. The majority of the houses are brick built, the most common locally available building material in the early 19th century. Quite a lot of that brick has been painted. There is a smaller use of rendered brick, again painted in most cases. There are a couple of uses of clapboard.

f. The views throughout the area are limited, with St. Andrew’s forming a focus for some of them. This results in a strong sense of enclosure, of an almost intimate residential community.

g. Most of the streets were comparatively quiet with a small amount of car traffic and not a lot of pedestrian movement. There was on-road car parking in most of the streets and this did not especially enhance their character - it certainly creates visual dissonance.

h. The overall character of the area is of a succession of houses and streets mostly built within a small historical timeframe creating little visual noise. It is a settled residential community. Any exceptions to that have been created by the impedimenta of the 20th century in the form of increased vehicle movement, telegraph poles and wires, television aerials and excessive street signage, including a large number of redundant signposts.

2. The Character Appraisal

2.1. Overview

The Nelson Street Conservation Area comprises about 200 buildings. These include a church, a public house and a very small number of commercial premises. Located close to the town centre and the seafront, the area is popular with residents who speak of a strong community spirit. The area developed historically through the first half of the 19th century in response to housing need and supply and this creates a strong sense of coherence and continuity. Although there is a variety of architectural style and detailing this does not detract from the area's overall cohesion. Most of the streets are low rise terraces punctuated by slightly larger three storey houses. Although that sense of cohesion is very strong, the individuality of both houses and streets also creates variety.

The majority of the properties are well maintained, and with a few exceptions, there is a powerful sense of a community that enjoys living in close proximity to the town centre and the attractions of Deal seafront. The proximity of the area to the town's shops, restaurants, cafes and leisure facilities is highly valued by the residents. There was a small amount of evidence that some of the properties were holiday lets but historical research revealed that the philosophy of "build/buy to let" has always been part of the character of this area.

The gardens around St. Andrew's Church create a refreshing sense of space in what is otherwise a fairly narrow grid of domestic houses.

2.2. Duke Street

Buildings
Duke Street was largely constructed between 1806 and 1835. This comparatively short time span has resulted in a consistency and continuity in the style of the buildings. The houses are two or three storey and predominantly constructed from brick. Some brick has been painted and a few houses are rendered. There is one property fronted with clapboard. The houses define the space and the character of the street. They are primarily domestic dwellings although some of them have had commercial or social uses in the past. The overall condition of the houses is good although a small number would benefit from some renovation.

The roofs are largely Kent peg tiled. Valley gutters and parapet walls define the character of a large number of the properties. Shared downpipes add to the visual cohesion of the street. Doors come in a wide variety of styles but semi-circular arches and a repetition of fanlights also contribute to that cohesion. Some window sizes have been changed. Sash and casement windows are the norm. Two of the 41 properties have uPVC windows.

There is a reticence about the whole street - Pevsner might have been describing this street when he wrote: "a succession of domestic buildings each different with nothing making a visual noise".

Spaces
The houses are built up to the pavements and it is this that shapes the character of the street. The pavements on both the north and south sides of the street are even and well maintained. The road surface is patchy. It is a one way street with on-street parking on one side. The parking does create some visual dissonance. It is one of the busiest streets in the conservation area and the fact that the houses are built to the pavement emphasises the traffic noise impact.

Some of the street furniture negatively impacts on the space. The three streetlamps are all different in style and the one way street signs are in poor condition and a visual distraction. There are a number of TV aerials fixed to the front of properties. The telephone wires are visible but on the whole have a harmonious feel.

Views and Landscape
St Andrew's Church creates a focal point to the streetscape looking from east to west. This long straight view and the consistency of the architecture make for a very harmonious urban character. In Duke Street there is no significant roofscape viewed from the ground.

Ambience
The character of the street is defined by two rows of domestic houses built within a short historical timeframe. The vast majority are family houses and the overwhelming impression is of a settled residential community. There is little in the way of trees or plants. It is a reasonably tranquil street although there may be increased traffic flows at certain times of the day. There is a licenced public house in the street and that inevitably has some impact on noise levels at certain times.

2.3. Nelson Street

Buildings

Nelson Street was largely constructed between 1811 and 1835. The Nelson Chapel was built in 1814 and is now a grade II listed domestic residence. A bungalow was built in 1909. With two exceptions the houses are built to the pavement and that is what defines the space. The houses are predominantly two storeys with a small number of ~~three storeys~~ **two storeys with basement**. The main construction material is brick which in a significant number of cases has been painted. A small number have been rendered. The majority of the houses have slate roofs although the earliest buildings, constructed between 1811 and 1814 have Kent peg roofs. Valley gulley's and shared downpipes are a feature of the roofscape.

It was noted that 16 out of 41 properties had uPVC windows. There was a range in the style of windows and bow windows featured in a few of the houses. One or two windows had been reconfigured. The doors appear in a wide variety of styles with semi-circular arches giving some continuity and consistency to the street. There were a number of additional decorative features and in one instance features had been added that were out of character with the period.

Some properties had undergone alterations with an additional storey being added. The whole street consists of domestic residences, including the Nelson Chapel. Historically there is evidence of properties being built to let and this usage appears to continue. One property was in a state of serious disrepair.

Spaces
Nelson Street is a straight street built mainly to the pavement. There are, however, a few features that create a different kind of space. The space around the former Nelson Chapel opens up the street and creates limited views to a neighbouring street. One property has a small front garden and there are gardens in front of two cottages in Garden Alley which leads off the street. Dominating the intimate space in Garden Alley is a large monkey puzzle tree located within the rear garden of a dwelling on Water Street. Trees are few and far between in the conservation area, and the monkey puzzle is a rare feature, offering visual respite from the densely built up streets.

The pavements are predominantly paving slabs which have been extensively patched, as has the road surface. The street has two matching street lamps. There are a large number of TV aerials attached to the front of roofs and this creates a discordant note in the street. There are redundant posts for street signage.

There is parking down one side of the street but there appears to be very low levels of vehicle movement and this gives the street a quiet domestic character.

Views and Landscape
The street has one long straight view with not a high level of harmony in the overall street scape. The chimney stacks dominate the roof line and on the east side of the street this creates a sense of overbalance.

Ambience
The overwhelming character is of a quiet domestic street with minimal levels of road and pedestrian traffic. The domestic buildings define its essential character.

2.4. Water Street

Buildings
Unlike elsewhere in this conservation area Water Street is a gently winding street. It takes its name from the Waterworks that were established at the junction with Lower Street (now the High Street) by the Waterworks Act in 1699. The majority of the houses are built to the pavement but at the lower end of the north side small garden spaces to the front of the houses give a distinctive variety to the street. The houses, built between 1806 and the 1840s, are predominantly two storeys with a few ~~three storeys~~ **two storeys with basements, steps leading to the front entrance door and curved boundary walls between each property**. Although there is considerable variety in architectural style the street has continuity and coherence. One building (Duke House) is Grade II listed.

The houses are all built of bricks. There is a small amount of render, Artex and pebbledash and in a number of cases the brick has been painted. The roofs are a mixture of slates and Kent peg tiles. On the north side of the street the chimney stacks are imposing and create a dominant note in the street. There was one dominant pediment which seemed over heavy for the house's facade.

There were 15 of the 37 properties with uPVC windows but it was noted that in some cases they were of a more sympathetic design. There was considerable variation in style but the soldier arches above the windows made for a strong sense of continuity in the street. The doors, too, were very varied but the arches above them gave the same sense of rhythm and continuity.

All of the properties are now used as domestic residences but there were clues to previous commercial uses. Earlier uses as a bakery, a builders and undertakers and a marine store were reflected in the architecture. The overall condition of the properties was generally good.

Spaces

The small spaces in front of the houses at the lower north side extend the sense of space in the street. The steps up to the front doors, the curving walls leading down to gate pillars and the small spaces in front of the houses all contribute to that sense of space. A small courtyard to the south of the street also creates a pleasing interlude. The pavements are largely paving slabs but some use of tarmac was noted. There were four modern streetlights and one traditional one. The telegraph posts and wires appeared intrusive and there were a number of redundant metal signposts. There is parking down one side of the road but traffic seemed to be very low. Overall the street had a quiet domestic character.

Views and Landscape

The street slowly unfolds when viewed from the eastern end. There is little focus to the street and at the west end a rather ugly outbuilding detracts from the overall quality of the conservation area. TV aerials to the front of houses and poorly maintained chimney stacks also detract. However the overall streetscape is cohesive with the exception of the space at the west end of the street.

Ambience

Again this is a quiet domestic street with very low levels of pedestrian and motor traffic. A few architectural references to earlier commercial activity give some distinctiveness and add character. But it is the early 19th century domestic residences that define its essential character.

2.5. Princes Street

Buildings

Only part of Princes Street lies within the conservation area boundary; numbers 1 and 3 are Grade II listed. About a third of the street, which is very similar to the houses within the conservation area, lies outside of it. The houses are predominantly two storey cottages built to the pavement. A row of four cottages on the east side was built in 1925 as residences for the printing industry. On the west side of the street there are three double fronted houses. Most of the properties, built of brick, were constructed between 1830 and 1850. The houses are domestic residences and there is little residual evidence of previous commercial use although one was identified as having been a pork butcher.

There are a significant number of properties where the brick has been painted. The 1925 cottages appear to have their original render, some of it painted. The overall condition of the properties was more variable than in other parts of the conservation area.

There was uniformity about the roofs with a mixture of Kent pegs and slates. There were 14 of the 27 residences with uPVC windows, some of them of a more sympathetic design. The soldier arch over the windows again created a sense of uniformity as did the round arches over the doors. There was a mixture of door styles sometimes creating a lack of harmony. This street does not show the same level of cohesion and continuity as other parts of the conservation area, which is particularly apparent with the later built cottages. The buildings in the street illustrate the way that developments over time can create a dissonance.

Spaces

The houses are built up to the pavements and this creates a narrow enclosed space. The pavements on both the east and west sides were in comparatively good repair and were constructed from paving slabs. The road surface was patchy. There is parking on one side of the road which creates some visual dissonance.

The street furniture also contributes to that dissonance. The street lights are modern in design and do little to enhance the street. TV aerials were less intrusive than in some other parts of the conservation area. The telephone lines were visible but created a better sense of harmony than in other parts of the area.

Views and Landscape

The straight view with houses built up to the pavement creates a sense of coherence.

Ambience
The vast majority of the houses are small domestic residences and the overall impression is of a quiet residential community. Little traffic movement was evident and there was little evidence of intrusive noise.

2.6. Robert Street

Buildings
The east and west sides of Robert Street vary in character. Only two properties on the east side fall within the conservation area boundary. On the west side there are properties built in the first half of the 19th century built to the pavement and there is also a terrace of houses built in 1977. On the east side, but lying outside of the conservation area, is a similar terrace of 20th century houses.

The overall effect lacks continuity. The size and scale of the properties is appropriate to the street. Most are brick built but with some use of render and pebbledash. The row of modern houses on the west side replaced a large house which had been the Bell Inn. A property on the east side was the Alhambra Music Hall historically and a property on the corner of Robert Street and Water Street had been the Duke of Wellington public house; all the properties are now domestic residences.

There is little sense of continuity in the roofscape on the east side but the west side has coherence first in the terrace of 20th century houses and in the group of 19th century properties. There were 11 of the 15 houses with uPVC windows. In one case changes to the shape of the windows had been achieved by very poor render. The doors in the 20th century terrace created a pleasing sense of unification. This street had quite a high proportion of houses where the condition of the facades was not good.

Spaces
A small car park to the west of the street and a large vista with gardens outside the conservation area creates a good sense of space in the middle of the street. The railings to the front of the modern terrace, often enclosing flower pots and shrubs, also added to the sense of space. With only a small number of the houses built up to the pavement this creates a very different sense of space to some of the other streets in the area. The use of tarmac for the pavement surfaces, a very patchy road and cars parked on both sides of the road did little to enhance the character of this street. The two streetlights on iron brackets and three telegraph poles also contributed to the lack of visual harmony.

Views and Landscape
The streetscape is varied and muddled with disrupted views. The view out of the east side of the street towards Clarence Place on the High Street is pleasing. It adds to the character of the conservation area without being part of it.

Ambience
The character of the street is defined by groups of 19th and 20th century houses all of which are domestic residences. Again the character is of a settled domestic community with little pedestrian or traffic disruption. There were six properties within the street that were not within the conservation area, it was very difficult to understand why that was the case.

2.7. St Andrew's Church, St Andrew's Road, Union Road, West Street

Buildings

Following the demolition of the late Eighteenth Century Deal Workhouse, St. Andrew's Church was built 1848-1850 and consecrated in 1850, it is Grade II listed. The church, built of Caen stone, was a response to the economic depression that affected Deal after the Napoleonic wars and the increasing poverty among the boatmen of Deal. It is still popularly known as "The Boatmen's Church". The church is a prominent and dominant feature on the western side of the conservation area. The building suffered from some Second World War damage; earlier photographs show a slate roof but it is now tiled. A window to the back of the church has been filled with flint stones. **The west boundary wall to St Andrew's Church is shown on the tithe map and is possibly related to the Workhouse.**

The original Queen Anne Rectory stood on the corner of Union Road and the High Street. It was demolished in 1964 and replaced by a brick built "executive style" house adjacent to the church sometime in the 1960's. Unusually this was built on land already consecrated for burials. The site for both the church and the rectory was the original site of the Deal workhouses.

A small portion of St. Andrew's Road immediately adjacent to the church gates falls within the conservation area boundary. The houses, which vary from a late 18th century cottage to small terraces built in the 1880's are largely brick built. Some of the brick has been painted. There were five of the ten houses with uPVC windows varying in quality and design. The doors are also diverse. The condition of the houses varied considerably especially on the west side of the road.

There are two buildings in Union Road within the conservation area boundary. The first is in use as a veterinary surgery. Originally a brick built 19th century commercial building it has been developed on both sides with 20th century brick extensions and garages. The second is a large garage on the corner of St. Andrew's Road and Union Road.

The buildings in West Street that fall within the conservation area boundary are varied. On the west side of the street there is Stafford Terrace, probably mid 19th century, a small commercial building and a small Victorian cottage. On the east side there is a range of small cottages from the late 18th and early 19th century, a number of small early 19th century cottages hidden behind high garden walls, a pair of 1980s houses and a very substantial commercial building which probably dates from the late 18th century. Some of the properties, especially Stafford Terrace, have been rendered but the dominant material is brick.

In total there were 16 of the 24 properties with uPVC windows varying in quality and design. 99-109 (odd numbers) West Street has a gently curving roofline with a

continuous Kent peg tile roof which is particularly pleasing. The windows in the large commercial building at the north-west boundary of the area have all been replaced with uPVC type.

Spaces
The gardens surrounding St Andrew's Church create a very pleasing formal space in a conservation area that has few open spaces. There are also a higher percentage of gaps between buildings in this part of the conservation area in marked contrast to the houses built up to the pavement in other parts. The new railings, Calgary and seats that have been installed to the eastern frontage of the church grounds in 2014-15 are a major enhancement of the conservation area.
The pavements in these streets were fairly well maintained paving slabs with the exception of West Street where tarmac had been laid over extensive areas of pavement. This did little to improve the appearance of a conservation area. The roads were reasonably well maintained.

There were a significant number of redundant sign posts which did little to enhance the area as well as a very poor metal bollard at the corner of St. Andrew's Road and Union Road.

Views and Landscape
St. Andrew's Church forms a focal point for this part of the conservation area and figures in a varied range of views from different parts of this conservation area. Both the streetscape and the roofscape are more varied in each part of this section of the conservation area partly because of the way in which the boundary is drawn. This is especially the case on West Street.

Ambience
The churchyard affords an oasis in the middle of a built up urban area. Although there is more road traffic in West Street than other parts of the conservation area, the other roads had a sense of domestic quiet and calm. The activities of the area also offer more variety with worship at the church, commercial activity in Union Road and West Street as well as a significant and varied number of domestic residences. All these activities add additional significance to the overall character of the conservation area.

3. Management Plan

3.1. Vulnerabilities and Negative Features

a. Although the overall standard of maintenance was good there was some evidence of a few properties not reaching the standards expected of a conservation area. In a few cases there was also evidence of building work not consistent with the historic character of the property. There was only one property, located in Nelson Street, which was considered to diminish the quality of the conservation area.

b. There are a number of buildings that are not listed but are of some architectural or historic interest.

c. The lack of planning control over the replacement of windows and doors was very evident. The very high number of uPVC windows is a matter of concern. In some cases the windows had been replaced in a sympathetic manner but there were a significant number of replacements where the style was completely alien to the historic character of the property. This also applied to a lesser degree to the replacement of doors.

d. There were a few examples where unsympathetic features had been added. These distracted from the historic and heritage significance of the property.

e. The majority of street lights were modern and the disparity of styles detracted from the character of a conservation area. In some streets the television aerials on the front of buildings spoiled the roofline. There was a refreshing absence of visible satellite antenna.

f. A significant number of disused signposts did nothing to enhance the character of the area. On the corner of St. Andrew's Road and Union Road a metal bollard, in very poor condition, was a visual eyesore.

g. The pavements and roads were reasonably maintained although some residents would dispute this view. The exception was West Street where the use of tarmac diminished the character of the conservation area. This equally applied to small areas of pavement where paving slabs had been lifted and replaced with tarmac.

3.2. Recommendations

3.2.1. Extensions of Boundary

One of the tasks of this appraisal has been to review the conservation area boundary in order to ensure that those buildings in it justify their inclusion, and to see if it is appropriate to extend the boundary to include additional buildings.

This review confirms that there are no buildings currently within the conservation area which should be excluded from it, but that the boundary should be extended to include:

- Faber Villa, Robert Street – The building is of significant architectural and historical interest.
- Green area on Clarence Place adjacent to Faber Villa – This area enhances the setting of the conservation area but is not currently part of it.
- The remaining area in Princes Street to the junction with Ark Lane – The similarity in style to the rest of the street argues for its inclusion.

3.2.2. Tree Protection Order

To afford protection to the monkey puzzle tree located in the rear garden of Prospect Cottage, Water Street, and visible from Garden Alley from loss, a Tree Protection Order is recommended.

3.2.3. Heritage Assets of Local Importance

The Government's National Planning Policy Framework states that 'non-designated' (i.e. essentially locally-identified) heritage assets should be taken account of when considering planning applications. A Local List would enable the importance of undesignated local heritage assets to be taken into account in the processing of any planning applications which might have an impact on them or their setting.

A Local List would include buildings, structures, landscape and archaeological features which are of local interest and have no statutory designation. For inclusion within the Local List, the Heritage Asset must comply with at least one of the following criteria set out within the DDC Land Allocations Local Plan (adopted January 2015):

- Historic Interest
- Architectural and Artistic Interest
- Social, Community and Economic Value

- Townscape Character

The following buildings are examples that could be identified as being Heritage Assets of Local Importance:

- Duke Street former Baptist chapel
- Nelson Street former Baptist chapel
- British School, Duke Street
- Le Chalet, Nelson Street
- 2 Princes Street

3.2.4. Article 4(1) Direction

All local authorities were given the power to impose an Article 4(1) Direction by the Town and Country Planning (General Permitted Development) Order 2015.

It is recommended that an Article 4(1) direction be implemented for the whole of this conservation area.

The regulations governing that Direction are set out in Appendix 1 of this ~~report~~ **appraisal**.

4. Appendices

4.1. Historical Development

Deal developed when the marshy shore became consolidated enough for building to start. Known as “the sea valley”, it was here, in the 16th century that three castles, Walmer, Deal and Sandown were built to protect the realm.

The original town had been on higher ground in Upper Deal. Lower Deal developed as countless ships sheltered in the Downs, an area of sea between the coast and the Goodwin Sands. The ships required both supplies and pilots and in turn that created the need for dwellings. The first mention of buildings on the beach is 1623 close to Deal Castle.

In 1699 the Waterworks was established at the junction of Water Street and Lower Street (now High Street), hence the name of the street.

In 1786 there were more than 750 houses in Lower Deal. The Napoleonic Wars meant that large numbers of service personnel, tradesmen and ancillary workers were resident in the town. The naval yard became the driver of the local economy. In the late 18th century the Archbishop’s lands, leased for farms and market gardens, was increasingly sold off for building.

The Pavement Act of 1791 gave a semblance of order to the layout, paving, lighting and draining of the streets.

Between 1801 and 1811 the population increased from 5420 to 7351. The Nelson Street conservation area is largely a response to that population growth. Between 1806 and 1840 a house building boom happened. Duke Street was named after Duke Hayman, the original owner of the land, and Nelson Street named after Vice Admiral Lord Nelson following the victory at Trafalgar.

The end of the Napoleonic wars meant the departure of many navy personnel and merchants: this resulted in high levels of social deprivation. **The Deal Workhouse was constructed in the late Eighteenth Century.** After 1834 the workhouses were full before the residents were moved to the Eastry Union in 1836. The workhouses were demolished in 1848 and St Andrew’s Church was built on the site and consecrated in 1850.

By 1851 most of what is known as the Nelson Street conservation area was built and the second half of the 19th century saw little further development.

In the 20th century two small rows of infill housing and a single bungalow were added to the area. In 1977 the area was designated a conservation area.

4.2. Map showing proposed boundary changes

To be inserted

4.3. Planning controls

4.3.1. Article 4(1) Direction

All local authorities were given the power to impose an Article 4(1) Direction by the Town and Country Planning (General Permitted Development) Order 1995.

The Article 4(1) Direction adopted by Dover District Council reinforces the Council's ability to protect the special character of a town. The Direction gives the District Council control over a variety of alterations to unlisted residences. Planning permission is required for changes to windows, doors, roof materials, and chimney stacks, and the construction of external porches, the provision and removal of walls and fences and the provision of hard standings.

These controls do not relate to the whole building, but only to those elevations which front a highway, waterway, or public open space, and which, therefore, affect the public face or faces of the building.

The best way of preserving the character of a building is to repair it using traditional materials. By using traditional materials there is no change to the external appearance and planning consent may not be required.

Direction 4(1) requires the submission of a planning application for the following items of work where the works front a highway, waterway or open space:

- The enlargement, improvement or other alterations of the house. This includes changing windows and doors.
- Any alterations to the roof, including roof lights, dormer windows, the substitution of clay tiles or natural slates with concrete or other materials.
- The erection or construction of a porch outside an external door.
- The provision within the curtilage of a house or any new buildings or any existing ones
- The provision of a hard surface e.g. for car parking in the front garden.
- The erection, alteration or removal of a chimney on the house or on a building within its curtilage.
- The erection, construction maintenance, improvement or alteration of a gate, fence or other means of enclosure.
- The painting of the external masonry (or other walling material) of any part of the house (or building or enclosure within the curtilage of the house). For the avoidance of doubt this does not include the routine painting of masonry or other walling material in the same colour.
- The installation, alteration or replacement of a satellite antenna on a house or within the curtilage of a house.

If the house is listed then Listed Building Consent for both external and internal alterations and extensions is required.

For further information consult the Dover District Council Planning website.

4.3.2. Tree Preservation Order

Local planning authorities have specific powers to protect trees by making tree preservation orders (TPOs). The order makes it an offence to cut down, top, lop, uproot, wilfully damage or wilfully destroy a tree without the permission of the Local Authority.

Trees are recognised as contributing to the character of a conservation area and are consequently afforded a certain level of protection. Where works are proposed to trees in a conservation area, the Local Authority must be given six weeks notice of the intent to carry out work. The Local Authority then has an opportunity to consider whether an order should be made to protect the tree. A conservation area appraisal can help identify which trees have particular importance to the character and appearance of a conservation area, and may be worthy of greater protection afforded by TPO status.

For further information consult the Dover District Council website.

4.4. Acknowledgement and references

Bibliography

The History and Topographical Survey of the County of Kent: Edward Hasted 1797-1801

History of Deal: Stephen Pritchard 1864

History of Deal: John Laker 1917

The Architecture of the British Isles: Sir Nikolaus Pevsner from 1940

Discovering Deal: Barbara Collins 1969

St Andrew's Church (The Boatmen's Church): Gregory Holyoake 1984

The Life and Times of a Small House in Deal: Andrew Sargent c1999

History of Deal: Gertrude Nunns 2006

The Old Pubs of Deal and Walmer: Steven Glover and Michael Rogers 2010

4.5. Glossary

Conservation Area is an area designated so that the planning authority can control changes within it. They can be defined as "Areas of special architectural or historic interest, the character or appearance of which it is desirable to preserve or enhance". Details can be found in the conservation pages of the DDC website.

Dover District Council (DDC) is the planning authority with responsibility for this conservation area. Their website is www.dover.gov.uk.

English Heritage in this ~~report~~ **appraisal** refers to the body officially known as the "Historic Buildings and Monuments Commission for England", which is the public body that looks after England's historic environment. It is now known as ***Historic England*** and their website is www.historicengland.org.uk.

Heritage Strategy is a DDC strategy which aims to enable them to achieve their objectives for the protection and enhancement of the historic environment. The strategy documents can be found in the conservation pages of the DDC website.

Kent County Council (KCC) is the authority with responsibility for, amongst other things, the highways in this conservation area. That responsibility includes road and pavement surfaces, signage and street lighting. Their website is www.kent.gov.uk.

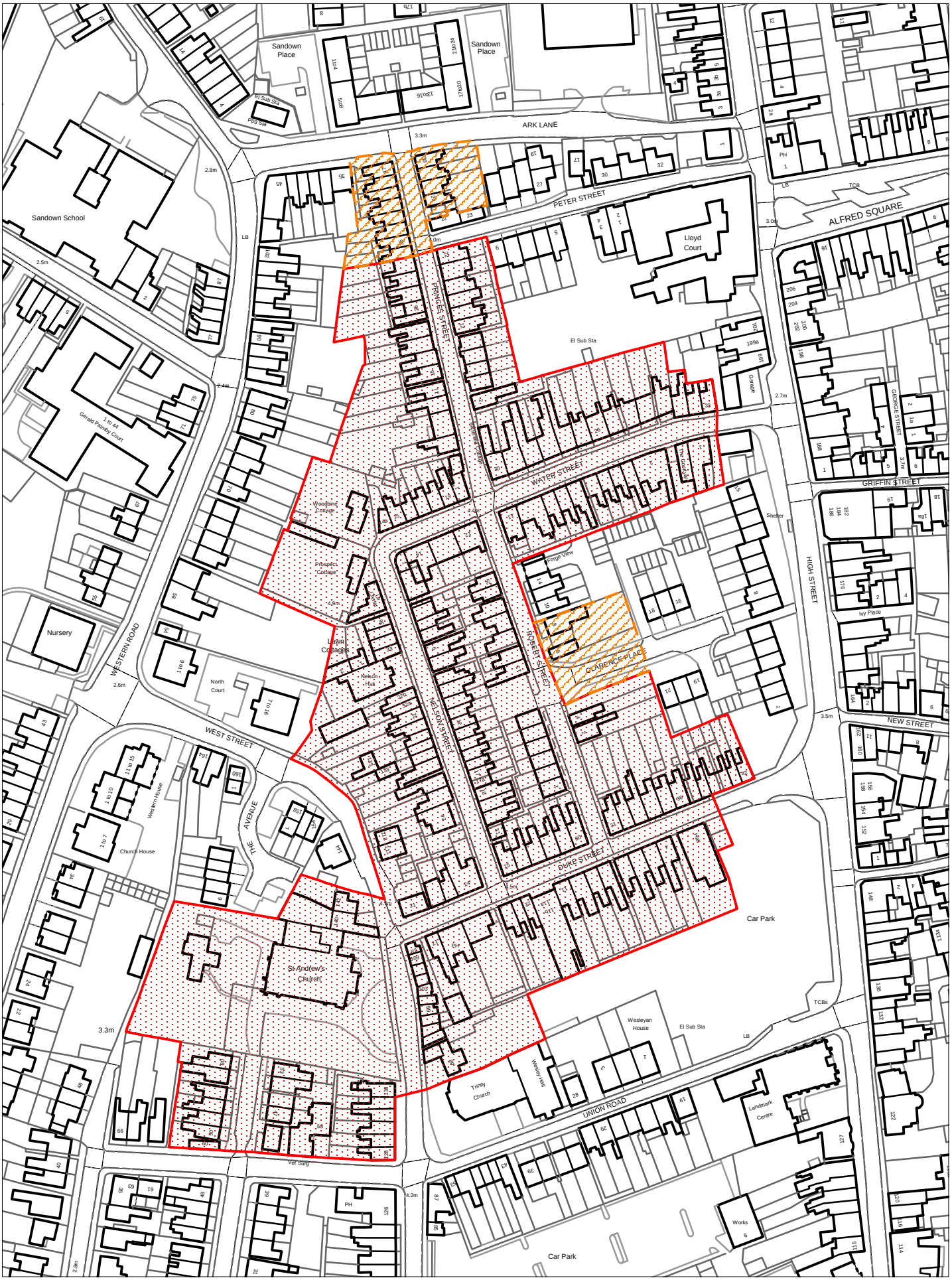
Listed Building is one designated as listed in the National Heritage List for England (NHLE). It marks and celebrates a building's special architectural and historic interest, and also brings it under the consideration of the planning system so that some thought will be taken about its future. There are three categories of listed building: Grade I, Grade II* and Grade II. Details are on the Historic England website.

National Planning Policy Framework is a key part of Government reforms to make the planning system less complex and more accessible, to protect the environment and to promote sustainable growth. Details can be found at the government's planning portal www.planningportal.gov.uk.

Non-designated Building refers to one which is not listed.

The Deal Society is the civic society for Deal and Walmer. Their website is www.thedealsociety.org.uk.

uPVC in this ~~report~~ **appraisal** refers to windows and doors, generally of aluminium construction, coated with plastic (usually white).



Existing Conservation Area Boundary

Proposed extension to Conservation Area

N

Not to Scale

DOVER DISTRICT COUNCIL

Subject:	**FEES AND CHARGES 2017/18**
Meeting and Date:	**Cabinet – 9 January 2017**
Report of:	**Mike Davis, Director of Finance, Housing and Community**
Portfolio Holder:	**Councillor Mike Conolly, Portfolio Holder for Corporate Resources and Performance**
Decision Type:	**Executive Key Decision**
Classification:	**Unrestricted**

Purpose of the report: This report has been prepared in order to obtain formal approval for the levels of fees and charges (F&Cs) for the financial year 2017/18. These F&Cs have been included in the preparatory work on the draft budget for 2017/18 and require approval.

Recommendation:

1. Cabinet approve the Fees and Charges (F&Cs) for 2017/18 as set out in Appendices 2 and 5.3

2. Members agree that any F&Cs will be adjusted by Service Director and Portfolio Holder to comply with any subsequently received government guidelines (when they are received) without being the subject of a further report unless they are materially different from current charges, or have a material impact on the level of income.

3. Members approve the general principle that fees are set at an appropriate inclusive level, irrespective of VAT status, and that the VAT element within the overall fee level is then determined.

4. Members note the fees and charges approved by Licensing and Regulatory Committees (which includes the Planning Committee) set out in Appendices 3, 4, 5.1 and 5.2

5. Members agree that the Director of Governance can authorise variation of the CON29 Land Charges to take account of the prevailing VAT requirements.

1. Summary

The Council's constitution specifies that F&Cs shall be reviewed annually. In order to meet this requirement all Directors have been asked to review the F&Cs within their areas of responsibility (see checklist of issues to consider – Appendix 1) and to produce recommended levels for 2017/18. The fees and charges are tabulated in the further Appendices for consideration and/or approval by Members.

2. Introduction and Background

2.1 The level of Member approval required is dependent upon the types of F&Cs raised. In order to obtain appropriate approval the following reports have been prepared:

- Licensing Committee

  Report to the meeting on 30 November 2016 of all F&Cs to be set by the Licensing Committee.

- Regulatory Committee

  Report to the meeting on 1 November 2016 of all F&Cs to be set by the Regulatory Committee.

- Planning Committee

  Report (for information) to the meeting on 24 November 2016 of all F&Cs relevant to the Planning Committee.

- Cabinet

  Report to the meeting on 9 January 2017 of all F&Cs, but seeking specific approval of those F&Cs set by Cabinet.

2.2 Members are reminded that a framework of broad guidelines to be considered in formulating proposals for F&Cs is in place. This includes a checklist which has been circulated to all Service Directors and to all officers considering F&Cs so that a rigorous and consistent approach is taken. A copy is attached at Appendix 1.

2.3 As in previous years, in order to assist Members, the data on F&Cs has been tabulated into a standard format that has been used for Appendices 2 to 5.

2.4 The main points to note are set out below.

Detail and Narrative

These give a brief summary of the type of service being provided.

Set by Government

This indicates whether a charge is statutory or not. If a charge is statutory then it is effectively set by Government and although formal Member approval is still sought, there is little or no scope to make changes.

2016/17 Charge Inc VAT

The charge has been provided inclusive of VAT for two reasons. First, it shows what the customer will actually pay and is therefore more meaningful.

Second, charges for some services, especially those such as car parking, which are not simply a direct recovery of costs, are set at a level, inclusive of VAT, based on the appropriate market level. The VAT is therefore a deduction from the amount of charge retained by DDC and is not a key factor in determining the appropriate charge. Members are asked to approve this approach.

2017/18 Proposed Charge Inc VAT

This is the recommended charge for 2016/17 and will, subject to Members' approval, be included in the 2016/17 budget.

2017/18 Total Expected Income ex VAT

This gives a broad indication as to how much income DDC is expected to receive and has been included to provide Members with a sense of the relative importance of individual charges or group of similar charges. The more significant income streams (generating over £3k) have been highlighted in **bold** type.

In some cases, the level of use is very low, or infrequent, or the service has only recently been introduced and so no level of income has been included.

Comments

This provides Members with a brief explanation for the change. In some instances guidance is still awaited from Government as to the basis upon which F&Cs should be set. In these cases it has not always been possible to confirm a fee level, Member's approval is sought to enable officers to adopt such fees at or close to government directed levels without a further report.

3. Other Fees and Charges

3.1 The following F&Cs are not included in this report.

3.2 Housing Rents and Service Charges

Housing rents are approved by the Director of Finance, Housing and Community under delegated authority. They are largely prescribed by government and the Council has no real scope to determine rent levels.

Service charges (for both tenants and long term lease holders) are determined through statutorily prescribed consultation processes and the recovery of all allowable costs. As a result the Council has no real scope to determine service charges.

3.3 Car Parking

Car parking fees are the subject of specific reports from the Director of Environment and Corporate Assets.

4. Identification of Options

4.1 The recommended figures for consideration by Members are included in the Appendices. Members may approve these proposed figures.

4.2 Members may propose and approve alternative figures with reasons recorded for their decisions.

4.3 Those fees already approved by Licensing and Regulatory Committees are for information only.

5. Evaluation of Options

5.1 The recommended fees and charges take into account the need to maximise income at a time of challenging budget positions, while taking into account comparable charges at neighbouring authorities and what the market can bear.

5.2 Members should also take into account the checklist of issues to consider (at Appendix 1) when reviewing the fees and charges included in the subsequent Appendices

6. Resource Implications

See Appendices

7. Corporate Implications

7.1 Comment from the Director of Finance, Housing and Community (linked to the MTFP): Finance have been involved in the production of this report and have no further comment to add (VB).

7.2 Comment from the Solicitor to the Council: The Solicitor to the Council has been consulted in the preparation of this report and has no further comment to make.

7.3 Comment from the Equalities Officer: 'The report does not specifically highlight any equality implications, however in discharging their responsibilities members are required to comply with the public sector duty as set out in section 149 of the Equality Act 2010 http://www.legislation.gov.uk/ukpga/2010/15'

7.4 Other Officers (as appropriate):

8. Appendices

Appendix 1 – F&C checklist
Appendices 2.1 – 2.5 – F&C for which Cabinet approval is sought
Appendices 3.1 – 3.2 – F&C to be approved by Licensing Committee
Appendices 4.1 - 4.2 – F&C to be approved by Regulatory Committee
Appendices 5.1 – 5.3 – Planning application fees

Contact Officer: Mike Davis, Director of Finance, Housing and Community

Fees and Charges Checklist

Corporate and Service Objectives Are links made between charges and our corporate and service objectives and are we able to use charges to help deliver these objectives?
Users of the Service Is there sufficient understanding of our service users and their needs and wishes? Have we considered different pricing to specific target groups and has the potential impact of charges or the changes to existing charges been assessed? Ensure that you consider the potential diversity and equality issues and where necessary consider and document any issues and mitigation.
Comparison with other providers Is there a complete picture of competition and providers of similar services – including other Local Authorities?
Consultation Has the relevant Portfolio holder been consulted and do charges meet with their aspirations and requirements? Is wider community consultation appropriate for any of your charges? Has it been undertaken?
Performance Management Are the principles for charges clearly defined and are clear targets set and monitored. Do we have a clear picture of what is a success?
Financial Considerations Is the charge at a level to fully recover all costs or if is subsidised - why? Have we considered all services for which we can / should charge a fee? Are there any fees that we charge, that have not been included in the schedule? Are we being radical in our approach to charging and are our charges cost effective?
Corporate Income Policy Please ensure you adhere to the main principals of the Corporate Income Policy when setting your fees and charges.
Legal Considerations and Other Guidance Does the Council have the power to levy the charges. Is there any ministerial or other guidance that should be taken into account?
Customer Access Review Consider whether the CAR for your service includes any issues for specific fees.

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % change**	**Reasons for Change in Charges and/or income**
	Building Control - R. Walton - M. Leggatt - Cllr Bartlett							
1	General	Building Regulations general enquires	N	£53	£53.00	**£100**	0%	
2	General	Solicitors enquiries & other specialist advice	N	£26.65	£26.65		0%	
3	General	Where customer specifies the relevant application reference and no research is required, the charge for a certified true copy	N	£5	£5.00		0%	
4	General	Production of Standard Assessment Procedure (SAP) - energy ratings	N	£303.00	£303.00	**£1,500**	0%	reduction in BC staff has meant that there is insufficient resource to service many SAP applications
5	General	Fees for Building Regulations Fee Earning Work as defined by Building (Local Authority Charges) Regulations 2010. Copy of charges scheme available in Building Control - fees sheets available on internet	N		Various	**£280,000**	0%	
6	General	Structural design	N		£0.00	**£0**	0%	Service suspended following departure of Senior BCS (replaced with part qualified BCS)

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % change**	**Reasons for Change in Charges and/or income**
7	General	Administration/professional charges for dealing with dangerous structures	N	£53	£0.00	**£200**	-100%	Dangerous structure notifications number 20 to 30 a year - vast majority resolved without need to charge.
	Dover Museum - R Walton - J Iverson - Cllr Watkins							
8	General	Adults	N	£4.50	£0.00		-100%	This element of fees and charges was subject to an agreement to allow frree entry to the museum for a trial period. This will be reviewed at the completion of that period. The income loss was offset by adjustments in internal budgets and by a grant from Dover Town Council.
9	General	Children	N	£3.20	£0.00		-100%	
10	General	OAP	N	£3.20	£0.00		-100%	
11	General	Family Day	N		£0.00		0%	
12	General	Family Ticket (2 adults, 2 children)	N	£11.50	£0.00		-100%	
13	General	Schools	N	£3.50	£0.00		-100%	
14	General	Schools Service: 2 hour workshop	N	£4.50	£5.00	**£18,000**	11%	Reflects increased cost of external providers
15	General	Talks and artefact handling	N	£3.50	£4.00		14%	
16	General	World War Two Festival	N	£5.50	£6.00		9%	
17	General	Roman/Victorian/Tudor Festivals	N	£5.50	£6.00		9%	
18	General	Curator talks (at Dover Museum)	N	£175.00	£200.00	£500	14%	
19	General	Talks (at Dover Museum) Non-DDC Area	N	£3.50	£3.50		0%	
20	General	Curator talks (other venues)	N	£175.00	£200.00		14%	
21	General	Photo repro stills - TV, film Video	N	£40.00	£48.00		20%	Prices have remained static since 2015 and do not reflect current costs
22	General	Photo repro stills - TV, film Video	N	£68.50	£82.20		20%	Prices have remained static since 2015 and do not reflect current costs

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % change**	**Reasons for Change in Charges and/or income**
23	General	Photo repro stills - books/periodicals - commercial	N	£28.50	£34.20		20%	Prices have remained static since 2015 and do not reflect current costs
24	General	Photo repro stills - books/periodicals academic and local history	N	£11.50	£13.80		20%	Prices have remained static since 2015 and do not reflect current costs
25	General	Photo repro stills - newspapers - local and regional	N	£23.00	£27.60		20%	Prices have remained static since 2015 and do not reflect current costs
26	General	Photo repro stills - newspapers - national	N	£40.00	£48.00		20%	Prices have remained static since 2015 and do not reflect current costs
27	General	Photo repro stills - exhibition commercial	N	£23.00	£27.60		20%	Prices have remained static since 2015 and do not reflect current costs
28	General	Photo repro stills - exhibition non commercial	N	£13.75	£16.50	£1,200	20%	Prices have remained static since 2015 and do not reflect current costs
29	General	Film and video broadcast - regional one use	N	£3.45	£4.14		20%	Prices have remained static since 2015 and do not reflect current costs
30	General	Film and video broadcast - regional continuing use	N	£5.75	£6.90		20%	Prices have remained static since 2015 and do not reflect current costs
31	General	Film and video broadcast - network one use, one country	N	£8.00	£9.60		20%	Prices have remained static since 2015 and do not reflect current costs
32	General	Film and video broadcast - network continuing use, one country	N	£11.50	£13.80		20%	Prices have remained static since 2015 and do not reflect current costs
33	General	Film and video broadcast - network continuing use, EC region	N	£14.25	£17.10		20%	Prices have remained static since 2015 and do not reflect current costs
34	General	Film and video broadcast - network continuing use, world	N	£18.25	£21.90		20%	Prices have remained static since 2015 and do not reflect current costs
35	General	Film and video broadcast - commercials etc. (world)	N	£36.50	£43.80		20%	Prices have remained static since 2015 and do not reflect current costs

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % change**	**Reasons for Change in Charges and/or income**
36	General	Cost of Preparing and sending images Print	N	£8.30	£9.96		20%	Prices have remained static since 2015 and do not reflect current costs
37	General	Cost of Preparing and sending Film and video	N	£20.80	£24.96		20%	Prices have remained static since 2015 and do not reflect current costs
38	General	Cost of preparing and sending stills	N	£20.80	£24.96	£300	20%	Prices have remained static since 2015 and do not reflect current costs
39	General	Cost of preparing and sending digital images	N	£5.20	£6.24		20%	Prices have remained static since 2015 and do not reflect current costs
40	General	Cost of preparing and sending digital images on CD	N	£10.40	£12.48		20%	Prices have remained static since 2015 and do not reflect current costs
41	General	Developing/printing 7x5	N	£6.85	£8.22		20%	Prices have remained static since 2015 and do not reflect current costs
42	General	Developing/Printing 10x8	N	£9.15	£10.98		20%	Prices have remained static since 2015 and do not reflect current costs
43	General	Developing/printing 12x10	N	£11.40	£13.68		20%	Prices have remained static since 2015 and do not reflect current costs
44	General	Handprint 10x8	N	£22.80	£27.36	Negligible income expected	20%	Prices have remained static since 2015 and do not reflect current costs
45	General	Handprint 12x10	N	£29.70	£35.64		20%	Prices have remained static since 2015 and do not reflect current costs
46	General	Handprint 16x12	N	£36.50	£43.80		20%	Prices have remained static since 2015 and do not reflect current costs
47	General	Handprint 20x16	N	£45.80	£54.96		20%	Prices have remained static since 2015 and do not reflect current costs
48	General	Photocopy A4	N	£0.25	£0.30	£75	20%	Prices have remained static since 2015 and do not reflect current costs
49	General	Photocopy A3	N	£0.35	£0.42		20%	Prices have remained static since 2015 and do not reflect current costs

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % change**	**Reasons for Change in Charges and/or income**
50	General	Film and video non-broadcast Educational continuing use world (Rights)	N	£3.45	£4.14	£150	20%	Prices have remained static since 2015 and do not reflect current costs
51	General	Film and video non-broadcast corporate non theatrical continuing use world (Rights)	N	£5.75	£6.90		20%	Prices have remained static since 2015 and do not reflect current costs
52	General	Theatrical shorts non broadcast less than 60 minutes (Rights)	N	£14.25	£17.10		20%	Prices have remained static since 2015 and do not reflect current costs
53	General	Theatrical films non broadcast longer than 60 minutes	N	£23.00	£27.60		20%	Prices have remained static since 2015 and do not reflect current costs
54	General	Digital Commercial Low res email (Rights)	N	£1.15	£1.38		20%	Prices have remained static since 2015 and do not reflect current costs
55	General	Digital Commercial High Res email (Rights)	N	£6.90	£8.28		20%	Prices have remained static since 2015 and do not reflect current costs
56	General	Digital Commercial Rescan email (Rights)	N	£9.20	£11.04		20%	Prices have remained static since 2015 and do not reflect current costs
57	General	Digital Commercial Internet single use email (Rights)	N	£91.25	£109.50		20%	Prices have remained static since 2015 and do not reflect current costs
58	General	Digital Commercial Exhibition (Rights)	N	£22.80	£27.36		20%	Prices have remained static since 2015 and do not reflect current costs
59	General	Digital Commercial Publication (Rights)	N	£28.20	£33.84		20%	Prices have remained static since 2015 and do not reflect current costs
60	General	Digital Commercial Newspaper National (Rights)	N	£40.00	£48.00		20%	Prices have remained static since 2015 and do not reflect current costs

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % change**	**Reasons for Change in Charges and/or income**
61	General	Digital Commercial Newspaper Regional (Rights)	N	£22.80	£27.36		20%	Prices have remained static since 2015 and do not reflect current costs

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % change**	**Reasons for Change in Charges and/or income**
	Environmental Health - R. Walton - D. Croucher - Cllr Bartlett							
62	Unsound Food Certificates	Not exceeding 1 metric tonne	N	£103.00	£103.00	£309	0%	Plus disposal charge
63	Unsound Food Certificates	Exceeding 1 metric tonne	N	£209	£209	£418	0%	Plus disposal charge
64	Port Health	Ship Sanitation Certificate	Y			**£10,000**	0%	Fees between £80 and £600 varies depending on tonnage and passenger capacity
65	Port Health	The Plastic Kitchenware (Conditions on Imports from China) (England) Regulations 2011	Y	£15	£15		0%	Documentary Check A
66	Port Health	The Plastic Kitchenware (Conditions on Imports from China) (England) Regulations 2011	Y	£50	£50	£0	0%	Documentary Check B
67	Port Health	The Plastic Kitchenware (Conditions on Imports from China) (England) Regulations 2011	Y	£100	£100		0%	Sampling Check plus £45 Courier (if required) plus analyst fees
68	Port Health	DPI Imported Food Examinations. Commission Implementing Regulation (EC) No 884/2014. (Previously (EC) No 1152/2009)	Y	£15	£15		0%	Documentary Check A
69	Port Health	DPI Imported Food Examinations. Commission Implementing Regulation (EC) No 884/2014. (Previously (EC) No 1152/2009)	Y	£50	£50	**£5,000**	0%	Documentary Check B

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % change**	**Reasons for Change in Charges and/or income**
	Environmental Health - R. Walton - D. Croucher - Cllr Bartlett							
70	Port Health	DPI Imported Food Examinations. Commission Implementing Regulation (EC) No 884/2014. (Previously (EC) No 1152/2009)	Y	£100	£100		0%	Sampling Check plus £45 Courier (if required) plus analyst fees
71	Port Health	DPE Imported Food Examinations. Commission Implementing Regulation (EC) No 669/2009	Y	£50	£50	£0	0%	Documentary Check
72	Port Health	DPE Imported Food Examinations. Commission Implementing Regulation (EC) No 669/2009.	Y	£100	£100		0%	Sampling Check plus £45 Courier (if required) plus analyst fees
73	Port Health	Catch Certificates IUU Regs - Council Regulation (EC) No. 1005/2008	Set by APHA	£40	£40		0%	Endorsement of Cert up to 5 certs
74	Port Health	Catch Certificates IUU Regs - Council Regulation (EC) No. 1005/2008	Set by APHA	£60	£60		0%	6-10 certs
75	Port Health	Catch Certificates IUU Regs - Council Regulation (EC) No. 1005/2008	Set by APHA	£70	£70		0%	11-20 certs
76	Port Health	Catch Certificates IUU Regs - Council Regulation (EC) No. 1005/2008	Set by APHA	£80	£80	£500	0%	21+certs

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % change**	**Reasons for Change in Charges and/or income**
	Environmental Health - R. Walton - D. Croucher - Cllr Bartlett							
77	Port Health	Catch Certificates IUU Regs - Council Regulation (EC) No. 1005/2008	Set by APHA	£20	£20	£500	0%	Bilateral Agreements Cert for up to 5 certs
78	Port Health	Catch Certificates IUU Regs - Council Regulation (EC) No. 1005/2008	Set by APHA	£35	£35		0%	6-10 certs
79	Port Health	Catch Certificates IUU Regs - Council Regulation (EC) No. 1005/2008	Set by APHA	£45	£45		0%	11-20 certs
80	Port Health	Catch Certificates IUU Regs - Council Regulation (EC) No. 1005/2008	Set by APHA	£55	£55		0%	21+ certs
81	Organic Food Certificates	Organic Products (import from Third Countries Regulations 2003)	Y	£45	£45	**£11,500**	0%	
82	Export Certificates	The Natural Mineral Water, Spring Water and Bottled Drinking Water (England) Regulations 2007 as amended	N	£50	£50	£0	0%	
83	Dog Control	Removal of stray dogs to kennels	Y	£25	£25		0%	
84	Dog Control	Out of hours Dog Collection	N	£40	£40	**£4,500**	0%	Increase based on income from last year.

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % change**	**Reasons for Change in Charges and/or income**
	Environmental Health - R. Walton - D. Croucher - Cllr Bartlett							
85	Dog Control	Kennelling fee per calendar day (up to a maximum of seven days)	N	£12.50	£12.50		0%	
86	Private Water Supplies	Risk Assessment		£500	£500	£0	0%	Hourly rate x officer time. Maximum fee £500.
87	Private Water Supplies	Sampling	Y	£100	£100	£0	0%	Hourly rate x officer time. Maximum fee £100.
88	Private Water Supplies	Investigation	Y	£100	£100	£0	0%	Hourly rate x officer time. Maximum fee £100.
89	Private Water Supplies	Granting an Authorisation	Y	£100	£100	£0	0%	Hourly rate x officer time. Maximum fee £100.
90	Private Water Supplies	Analysing a Sample under Reg 10	Y	£25	£25	£0	0%	
91	Private Water Supplies	Analysing a sample (Check Monitoring)	Y	£100	£100	£0	0%	Hourly rate x officer time. Maximum fee £100.
92	Private Water Supplies	Analysing a Sample (Audit monitoring)	Y	£500	£500	£0	0%	Hourly rate x officer time. Maximum fee £500.
93	Contaminated Land Enquiry	Up to 250m distance	N	£73	£32	£200	-56%	Hourly rate for officer time. Minimum fee 1 hour

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % change**	**Reasons for Change in Charges and/or income**
	Environmental Health - R. Walton - D. Croucher - Cllr Bartlett							
94	Contaminated Land Enquiry	Up to 500m distance	N	£142	£92	£200	38%	Hourly rate for officer time. Minimum fee 1 hour.
95	Environmental Protection Act 1990 - Air Pollution	Initial Application Fee (Standard)	Y			£0		Charges advised by DEFRA
96	Environmental Protection Act 1990 - Air Pollution	Substantial Changes Fee (Standard) including partial transfer and surrender fees for LA-IPPC	Y			£0		
97	Environmental Protection Act 1990 - Air Pollution	Substantial Changes Fee (Sections 10 and 11)	Y			£0		
98	Environmental Protection Act 1990 - Air Pollution	Annual Subsistence Charge (Standard)	Y			**£10,000**		
99	Public Health funerals	Officers admin fees in arranging funeral.	N	Maximum of £250	Maximum of £250	**£500**	N/A	Hourly rate x officer time. Maximum fee £250.
	Recycling & Waste Collections - R. Walton - M. Pile - Cllr Kenton							
100	Domestic Recycling & Refuse Collection	Supply & Delivery of 140 litre bin	N	£34.99	£34.99	£1,050	0%	30
101	Domestic Recycling & Refuse Collection	Supply & Delivery of 180 litre bin	N	£47.35	£47.35	£1,421	0%	30
102	Domestic Recycling & Refuse Collection	Supply & Delivery of 240 litre bin	N	£46.65	£46.65	£1,400	0%	30
103	Domestic Recycling & Refuse Collection	Supply & Delivery of 360 litre bin	N	£73.55	£73.55	£2,207	0%	30
104	Domestic Recycling & Refuse Collection	Supply & Delivery of 660 litre bin	N	£246.99	£246.99	£7,410	0%	30

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % change**	**Reasons for Change in Charges and/or income**
	Environmental Health - R. Walton - D. Croucher - Cllr Bartlett							
105	Domestic Recycling & Refuse Collection	Supply & Delivery of 1100 litre bin	N	£275.35	£275.35	£8,261	0%	30
106	Domestic Recycling & Refuse Collection	Supply & Delivery of 55l Black Box or Blue Box	N	£8.35	£8.35	£251	0%	30
107	Domestic Recycling & Refuse Collection	Supply & Delivery of 23l Kerbside Caddy for food collections	N	£8.35	£8.35	£251	0%	30
108	Domestic Recycling & Refuse Collection	Supply & Delivery of 7l Kitchen Caddy for food collections	N	£4.80	£4.80	£144	0%	30
109	Domestic Recycling & Refuse Collection	Supply & Delivery of Container 'Launch Pack' (2 WB, 2 Food + Box)	N	£75.95	£75.95	£2,279	0%	30
110	Domestic Recycling & Refuse Collection	Green Waste Collections; Annual Subscription for up to 6 sacks	N	£39.95	£39.95	£199,750	0%	5000
111	Domestic Recycling & Refuse Collection	Green Waste Collections; Supply & Delivery of 60l Reusable Garden Waste Sack	N	£3.60	£3.60	£7,200	0%	2000
112	Domestic Refuse	Bulk Domestic Waste - Collection (charge for 5 items)	Y	£29.95	£29.95	£29,950	0%	1000
113	Domestic Refuse	Bulk Domestic Waste, Abortive Visit	Y	£29.95	£29.95	£150	0%	5
114	Domestic Refuse	Bulk Domestic Waste, Additional Items	Y	£5.00	£5.00	£50	0%	10
	Leisure Facilities - R. Walton - M. Leggatt - Cllr Bartlett							
115	Deal Pier Fishing	Daytime (08:00 to 22:00 hrs April-November, 08:00 to 18:00 hrs December-March) - adult	N	£6.00	£6.00		0%	

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % change**	**Reasons for Change in Charges and/or income**
	Environmental Health - R. Walton - D. Croucher - Cllr Bartlett							
116	Deal Pier Fishing	Daytime (08:00 to 22:00 hrs April-November, 08:00 to 18:00 hrs December-March) - concessions (unemployed, senior citizens, disabled and students (including under 16's))	N	£3.00	£3.00		0%	
117	Deal Pier Fishing	Daytime (08:00 to 22:00 hrs April-November, 08:00 to 18:00 hrs December-March) - hand lines	N	£1.45	£1.50		3%	
118	Deal Pier Fishing	Evening (17:00 to 22:00 hrs April-November, 13:00-18:00 hrs December to March) - adult	N	£4.30	£4.50		5%	
119	Deal Pier Fishing	Evening (17:00 to 22:00 hrs April-November, 13:00 to 18:00 hrs December-March) - concessions (unemployed, senior citizens, disabled and students (including under 16's))	N	£2.20	£2.30	**£37,500**	5%	Certain charges frozen, others raised between 0 and 5% in order to facilitate collection of fees and minimise change.
120	Deal Pier Fishing	Night Time (22:00 to 06:00 hrs) - adult	N	£8.40	£8.50		1%	
121	Deal Pier Fishing	Night Time (22:00 to 06:00 hrs) - concessions (unemployed, senior citizens, disabled and students (including under 16's))	N	£4.80	£5.00		4%	
122	Deal Pier Fishing	Combined 'Day and Night' Ticket - adult	N	£10.75	£11.00		2%	
123	Deal Pier Fishing	Combined 'Day and Night' Ticket - concessions (unemployed, senior citizens, disabled and students (including under 16's))	N	£7.05	£7.00		-1%	
124	Hire of Pier	Per night booking	N	£193	£200.00		4%	

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % change**	**Reasons for Change in Charges and/or income**
	Environmental Health - R. Walton - D. Croucher - Cllr Bartlett							
125	Sports - Parks and Recreation Grounds	Bowls: Season Ticket - Adult	N	£66	£67.00		2%	
126	Sports - Parks and Recreation Grounds	Bowls: Season Ticket - OAP	N	£66	£67.00		2%	
127	Sports - Parks and Recreation Grounds	Bowls: Season Ticket - Junior	N	£32.75	£33.50	**1500**	2%	Income figures estimated as collection rates under new management structure may vary
128	Sports - Parks and Recreation Grounds	Visitors green fees per game 21 ends (per game per person) per game (per set – 4 woods and 1 Jack)	N	£3.20	£3.30		3%	
129	Sports - Parks and Recreation Grounds	Football: Pitch Hire - Adult	N	£51.50	£53.00		3%	
130	Sports - Parks and Recreation Grounds	Football: Pitch Hire - Juniors	N	£21	£21.50		5%	Higher increase keeps charge simple
131	Sports - Parks and Recreation Grounds	Netball	N	£25.00	£26.00		4%	
132	Sports - Parks and Recreation Grounds	Tennis - Adult (per court per hour)	N	£4.80	£5.00		4%	
133	Sports - Parks and Recreation Grounds	Tennis - Junior (per court per hour)	N	£1.65	£1.70		3%	

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % change**	**Reasons for Change in Charges and/or income**
	Environmental Health - R. Walton - D. Croucher - Cllr Bartlett							
134	Sports - Parks and Recreation Grounds	Tennis - OAP (per court per hour)	N	£1.65	£1.70		3%	
135	Parks	Standard Hire Event	N	£156			-100%	Delete - too similar to small commercial combine categories
136	Parks	Deposit	N				0%	
137	Parks	Small Commercial/stnadard Event - Operating Day	N	£163	£170.00		4%	
138	Parks	Small Commercial Event - Non-Operating Day	N	£38	£40.00		5%	
139	Parks	Small Commercial Event - Deposit	N	£1,000	£1,000.00		0%	
140	Parks	Large Commercial Event - Operating Day	N	£530	£555.00		5%	
141	Parks	Large Commercial Event - Non-Operating Day	N	£84.50	£88.50	**£19,475**	5%	
142	Parks	Large Commercial Event - Deposit	N	£1,000	£1,000.00		0%	
143	Parks	Mobile Exhibition - Per Day	N	£75	£79.00		5%	

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % change**	**Reasons for Change in Charges and/or income**
	Environmental Health - R. Walton - D. Croucher - Cllr Bartlett							
144	Parks	Mobile Exhibition - Deposit	N	£200	£200.00		0%	
145	Parks	Community Event or Event run by a registered charity - per day	N	£45	£45.00		0%	
146	Parks	Community Event or Event run by a registered charity - per deposit	N	£200	£200.00		0%	
147	Parks	Use of parks for commercially run fitness and similar activities - fee per session	N	£15.00	£25.00		n/a	
148	Parks	Commemorative Trees	N	£375	£395.00		5%	
149	Parks	Memorial Benches administration fee	N	£210	£195.00	(Included in £157,500 below)	-7%	
150	Parks	Commemorative Plaques	N	£199	£200.00		1%	
151	**Cemetery - R. Walton - M. Leggatt - Cllr Bartlett**							
152	General	Maintenance	N	£51	£52.50		3%	
153	General	Maintenance and Planting	N	£107	£110.00		3%	
154	General	Purchase of Grave Space - Adult (This fee will be doubled for non residents)	N	£655	£675.00		3%	

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % change**	**Reasons for Change in Charges and/or income**
	Environmental Health - R. Walton - D. Croucher - Cllr Bartlett							
155	General	Purchase of Grave Space - Child under 12 years	N	£0	£0		0%	
156	General	Purchase of Cremation Grave/Ashes Plot (This fee will be doubled for non residents)	N	£185	£190.00		3%	
157	General	Use of Chapel	N	£151	£155.00		3%	
158	General	Garden of Remembrance - right to erect a tablet	N	£89	£91.00		3%	
159	General	Interment of Ashes (excluding caskets or urns)	N	£187	£192.00		3%	
160	General	Search in Burial Register (to be charged when time involved exceeds 1 hr)	N	£55	£57.50		5%	
161	General	Right to erect a memorial not exceeding 1.06 metres in height, 0.76 metres in width and 0.45 metres in depth	N	£169	£174.00		3%	
162	General	Vase not exceeding 0.30 metres in height or tablet not exceeding 0.25 metres (including a tablet for a stillborn child) with only the name or initials, date of death and age of person inscribed	N	£79	£81.00		3%	
163	General	Right to place on any flagstone, headstone, kerbstone, border stone, inscribed vase, tablet or monument, each further inscription	N	£71	£73.00	£157,500	2%	
164	General	Replacement of a headstone with a new headstone	N	£35	£40.00		14%	Current (2016/17) charge does not cover costs of the service

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % change**	**Reasons for Change in Charges and/or income**
	Environmental Health - R. Walton - D. Croucher - Cllr Bartlett							
165	General	Right to place kerb - depending upon location within cemetery		£375	£385.00		3%	
166	General	Interment of cremated remains in any grave	N	£187	£192.00		3%	
167	General	Interment of a stillborn child or child under 6 months	N	£56	£57.00		2%	
168	General	Interment of a child exceeding 6 months but under 12 years	N	£245	£250.00		2%	
169	General	Interment of an adult or child exceeding 12 years: single depth - new grave	N	£810	£835.00		3%	
170	General	Interment of an adult or child exceeding 12 years: single depth - reopen	N	£630	£650.00		3%	
171	General	Interment of an adult or child exceeding 12 years: double depth - new grave	N	£930	£960.00		3%	
172	General	Interment of an adult or child exceeding 12 years: double depth - reopen	N	£785	£810.00		3%	
173	General	Interment of an adult or child exceeding 12 years: triple depth	N	£1,140	£1,175.00		3%	
174	General	Laying Down of Unsafe Memorials Or Making Memorials Safe	N	£108	£0.00		-100%	Delete - occurs on old graves, majority of occurrences the family are difficult impossible to trace hence not cost effective to pursue charge
175	General	One Off Contribution For Maintenance For Coffin Burials	N	£215	£222.00		3%	
176	General	One Off Contribution For Maintenance For Cremated Remains	N	£83.00	£85.00		2%	

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % change**	**Reasons for Change in Charges and/or income**
	Environmental Health - R. Walton - D. Croucher - Cllr Bartlett							
177	The above charges apply where the person to be interred is, or immediately before death was a resident in the Dover District Council area, or in the case of a stillborn child, where the parents (or one of them) are residents of the District.							
	Foreshore - R. Walton - M. Leggatt - Cllr Bartlett							
178	Beach Plot Charges	Walmer Plot	N	£320	£320.00	**£15,456**	0%	Fee will be held for 17/18 then 2% annual increase until 21/22 and 5 year licences granted to reduce admin.
179	beach Plot charges	Deal/Walmer commercial plot	N	£151	£151.00		0%	
180	Beach Plot Charges	St Margaret's Plot	N	£225	£231.00		3%	
181	Beach Plot Charges	Kingsdown Plot	N	£178	£183.00		3%	Omit 50% discount ramp replaced
182	Beach Plot Charges	Extra Boat on Plot	N	£78.50			-100%	Delete - Difficult to monitor limited income pick up on overall cost of plot
183	Beach Huts	St Margaret's Bay - Annual	N	£1,150	£1,185.00	**£16,590**	3%	
184	Beach Huts	The Endeavour Centre - Daily	N	£34.00	£35.00	**£140**	3%	
185	Sandwich Quay	Long stay moorings per m per day (minimum 3 months) - Residents	N	£3.20	£3.20	**£2,500**	0%	Left at 16/17 prices to encourage greater use of the quay so that it is a vibrant environment, prices are not below Kent market values given the offering.
186	Sandwich Quay	Long stay moorings per m per day (minimum 3 months) - Non-Residents	N	£5.00	£5.00		0%	
187	Sandwich Quay	Short Stay Moorings per day (maximum 28 days)	N	£10.00	£10.00		0%	Left at 16/17 prices to encourage greater use of the quay so that it is a vibrant environment, prices are not below Kent market values given the offering.

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % change**	**Reasons for Change in Charges and/or income**
	Environmental Health - R. Walton - D. Croucher - Cllr Bartlett							
188	Beach Huts	Beach Hut Plots Kingsdown	N	£450.00	£465.00	**£9,300**	3%	
189	Filming on DDC land	Fee - per day	N	£570.00	£600.00	**£3,000**	5%	
190	Filming on DDC land	Fee - per hour	N	£97.00	£102.00		5%	
191	Statutory Street Naming and Numbering	Registering a New Property Address	N	£130.00	£135.00	**£15,500**	4%	
192	Statutory Street Naming and Numbering	New Street or Building Comprising 2-10 units	N	£270	£280.00		4%	
193	Statutory Street Naming and Numbering	New Street or Building Comprising 11-20 units	N	£430	£440.00		2%	
194	Statutory Street Naming and Numbering	New Street or Building Comprising 21 + units	N	£440	£450.00		2%	For developments in excess of 20 units - fee will be £440 plus £10 fee for each unit in excess of 20 units . No maximum fee.
195	Statutory Street Naming and Numbering	Changing Street Name	N	£570	£585		3%	
196	Non Statutory Street Naming and Numbering	Administration Fee for undertaking Non Statutory Function Street Naming and Numbering	N	£55	£55.00		0%	Current charge covesr hourly charge out rate

				2016/17	2016/17	2016/17	2016/17	2016/17	2016/17	2017/18	2017/18		2017/18	2017/18		2017/18		2017/18	
	Detail	**Narrative**	**Vatable Y/N?**	**Proposed Amount of penalty if paid within 15 days**	**units / comments**	**Proposed Full amount of penalty - 14 days**	**Units / comments**	**Maximum penalty on conviction**	**Total Expected Income**	**Proposed Amount of penalty if paid within 15 days**	**Units / comments**	**Penalty Amount % change**	**Proposed Full amount of penalty - 14 days**	**Units / comments**	**Full Amount of Penalty % change**	**Maximum penalty on conviction**	**Maximum Penalty on conviction % change**	**Total Expected Income**	**Justification for charge levels**
	Environmental Health - R. Walton - D Croucher - Cllr Bartlett																		
197	S48 Anti-Social Behaviour, Crime & Policing Act 2014	Failure to comply with a Community Protection Notice	N	Not applicable. Dover District Council set the level of fines at the standard default level for each offence without an early payment option through its FPN Policy.		£100	Standard default levels as laid down in legislation (in accordance with DDC FPN Operational Policy)	£2500 in the case of an individual, unlimited in the case of a body	**£9,500**	Not applicable. Dover District Council set the level of fines at the standard default level for each offence without an early payment option through its FPN Policy.			£100	Standard default levels as laid down in legislation (in accordance with DDC FPN Operational Policy)	0%	£2500 in the case of an individual, unlimited in the case of a body	0%	**£9,500**	
198	S33 Environmental Protection Act 1990	Fixed penalty notice for fly-tipping											£400			Unlimited fine.			New power to issue FPNs for fly-tipping introduced in May 2016. Proposed level of £400 subject to approval by Cabinet.
199	S34 Environmental Protection Act 90	Failure to produce waste documents	N			£300		Unlimited on indictment, £5000 on summary					£300		0%	Unlimited on indictment, £5000 on summary	0%		
200	S5 Control of Pollution (amendment) Act 1989	Failure to produce authority to transport waste	N			£300		£5,000					£300		0%	£5,000	0%		
201	s47 Environmental Protection Act '90	Failure to comply with a waste receptacles notice (commercial)	N			£100		£1,000					£100		0%	£1,000	0%		
202	s46 Environmental Protection Act 1990	Failure to comply with a waste receptacles notice (domestic)	N			£60	Paid within 28 days	Recoverable as a civil debt					£60	Paid within 28 days	0%	Recoverable as a civil debt	0%		
203	S7 Health Act 2006	Smoking in a smoke free premises or vehicle	N	£30	Paid within 15 days	£50	Paid within 29 days	£200		£30	Paid within 15 days	0%	£50	Paid within 29 days	0%	£200	0%		
204	S7 Health Act 2006	Smoking in a vehicle with a person under the age of 18 present.								£30	Paid within 15 days		£50	Paid within 29 days		£200			Legislation introduced in October 2015.
205	S6 Health Act 2006	Failure to display no smoking signs in smoke free premises or vehicles	N	£150	Paid within 15 days	£200	Paid within 29 days	£1,000		£150	Paid within 15 days	0%	£200	Paid within 29 days	0%	£1,000	0%		
206	S4 Noise Act 1996	Noise from dwellings exceeding the permitted level (defined in the Act)	N	No longer applicable. Dover District Council set the level of fines at the standard default level for each offence without an early payment option through its FPN Policy		£100	Standard default levels as laid down in legislation (in accordance with DDC FPN Operational Policy)	£1,000		Not applicable. Dover District Council set the level of fines at the standard default level for each offence without an early payment option through its FPN Policy			£100	Standard default levels as laid down in legislation (in accordance with DDC FPN Operational Policy)	0%	£1,000	0%		
207	S4A Noise Act 1996	Noise from licensed premises exceeding the permitted level (defined in the Act)	N			£500		£5,000					£500		0%	£5,000	0%		
208	S6 Clean Neighbourhoods & Env Act 2005	Nuisance Parking (exposing vehicles for sale on a road or repairing vehicles on a road)	N			£100		£2,500					£100		0%	£2,500	0%		
209	S.88(1) Environmental Protection Act 1990	Litter	N			£75		£2,500					£75		0%	£2,500	0%		
210	Sch. 3A para 7. EPA '90	Unauthorised distribution of literature on designated land	N			£75		£2,500					£75		0%	£2,500	0%		
211	S.43 Anti-Social Behaviour Act 2003	Graffiti and fly posting	N			£75		£2,500					£75		0%	£2,500	0%		
212	S.2A Refuse Disposal (Amenity) Act 1978	Abandoning a vehicle	N			£200		£2,500					£200		0%	£2,500	0%		
213	S.73 CNEA '05	Failure to nominate key holder (within an alarm notification area) or to notify the LA in writing of nominated key holder's details	N			£75		£1,000					£75		0%	£1,000	0%		
214	S.3 Dogs (Fouling of Land) Act 1996	Failure to remove dog faeces forthwith	N	Legislation still in force but fouling now dealt with under Public Spaces Protection Orders. May be reintroduced if PSPOs rescinded or not renewed.															

				2016/17	2016/17	2016/17	2016/17	2016/17	2016/17	2017/18	2017/18		2017/18	2017/18		2017/18		2017/18	
	Detail	**Narrative**	**Vatable Y/N?**	**Proposed Amount of penalty if paid within 15 days**	**units / comments**	**Proposed Full amount of penalty - 14 days**	**Units / comments**	**Maximum penalty on conviction**	**Total Expected Income**	**Proposed Amount of penalty if paid within 15 days**	**Units / comments**	**Penalty Amount % change**	**Proposed Full amount of penalty - 14 days**	**Units / comments**	**Full Amount of Penalty % change**	**Maximum penalty on conviction**	**Maximum Penalty on conviction % change**	**Total Expected Income**	**Justification for charge levels**
	Environmental Health - R. Walton - D Croucher - Cllr Bartlett																		
215	The Public Space Protection Order (Dover District Council) 2014	Failure to comply with Public Space Protection Order	N	Not applicable. Dover District Council set the level of fines at the standard default level for each offence without an early payment option through its FPN Policy. The level of FPN was approved by Cabinet and Scrutiny in June 2015.		£75		£1,000		Not applicable. Dover District Council set the level of fines at the standard default level for each offence without an early payment option through its FPN Policy. The level of FPN was approved by Cabinet and Scrutiny in June 2015.			£75	Not applicable. Dover District Council set the level of fines at the standard default level for each offence without an early payment option through its FPN Policy. The level of FPN was approved by Cabinet and Scrutiny in June 2015.		£1,000	0%		

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % change**	**Reasons for Change in Charges and/or income**
	Legal - D. Randall - H. Rudd - Cllr Conolly							
216	General	Engrossments (Right to Buy – Leasehold Transactions)	N	£75	£120	£4,200	60%	
217	General	All charges for legal professional work being met by third parties	N	£205	**£205**	£4,100	0%	Per hour
	Land Charges - D. Randall - L. Cooke - Cllr Conolly							
218	General	Requisition for Search (LLC1)	N	£27.50	£27.50		0%	
219	General	Optional Printed Enquiry (in Part 2 of Con 29O)	N	£12.00	£12.00		0%	
220	General	Any Additional Enquiry submitted	N	£15.00	£15.00		0%	
221	General	Search in respect of any extra parcel of land	N	£13.00	£13.00		0%	
222	General	Existing Conveyancing Form (CON29)	N	£98.50	£98.50		0%	
223	General	Proposed New Conveyancing Form (CON29)	N				100%	
224	General	CON29 Q1.1(a,b,c,d,e,f,g,h,i)	N	£3.50	£3.50		0%	
225	General	CON29 Q1.1(j,k,l)	N	£6.00	£6.00		0%	
226	General	CON29 Q1.2	N	£2.00	£2.00		0%	
227	General	CON29 Q2.1(a,b,c,d)	N	£3.50	£3.50		0%	
228	General	Proposed New CON29 Q2.2. 2.3, 2.4, 2.5 (Refer to KCC)	N	£6.00	£6.00			
229	General	CON29 Q3.1	N	£2.00	£2.00		0%	

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % change**	**Reasons for Change in Charges and/or income**
230	General	CON29 Q3.2	N	£2.00	£2.00	£220,000 in total for Land Charges	0%	
231	General	New QuestionCON29 Q3.3(a,b,c)	N	£3.50	£3.50		0%	
232	General	CON29 Q3.4 (a,b,c,d,e,f)	N	£5.00	£5.00		0%	
233	General	CON29 Q3.5 (a,b)	N	£4.00	£4.00		0%	
234	General	CON29 Q3.6 (a,b,c,d,e,f,g,h,I,j,k,l)	N	£3.00	£3.00		0%	
235	General	CON29 Q3.7 Flood and coastal erosion added)	N	£18.00	£18.00		0%	
236	General	CON29 Q3.8	N	£4.00	£4.00		0%	
237	General	CON29 Q3.9 (a,b,c,d,e,f,g,h,I,j,k,l,m,n)	N	£2.50	£2.50		0%	
238	General	New Question CON29 Q3.10	N	N/A	N/A		100%	
239	General	CON29 Q3.11(a,b)	N	£4.00	£4.00			
240	General	CON29 Q3.12	N	£2.00	£2.00		0%	
241	General	CON29 Q3.13(a,b,c)	N	£5.00	£5.00		0%	
242	General	CON29 Q3.14	N	£3.00	£3.00		0%	
243	General	New Question CON29 Q3.15	N	£1.50	£1.50		100%	
244	General	CON29 Administration Fee plus Question fees	N	£18.00	£18.00		0%	£18 admin fee now charged for CON29O and additional questions submitted without a standard search

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % change**	**Reasons for Change in Charges and/or income**
245	General	Personal Search Land Charges Register	N	£0.00	£0.00		0%	Free
	Electoral Services - D. Randall - L. Cooke - Cllr Conolly							
246	Representation of the People Acts and the Electoral Administration Act	Purchase of Register of Electors and copies of Election documents	Y	£0.00	£0.00		0%	As per Statutory Instrument
	Miscellaneous - D. Randall - M. Weir - Cllr Conolly							
247	Access to Information and Data Protection Acts	Inspection of list of background papers	Y	£0.00	£0.00	£0.00	0%	Freedom of Information free up to 18 hour limit
248	Access to Information and Data Protection Acts	Inspection of each set of documents	Y	£2.50	£2.50	£0.00	0%	Freedom of Information free up to 18 hour limit
249	Access to Information and Data Protection Acts	Inspection of personal data	Y	£10.00	£10.00	£100.00	0%	Maximum fee Council can charge as per legislation
250	Access to Information and Data Protection Acts	Environmental Information Request	N	N/A	£32.00	£100.00	N/A	New Charge from 2017/18

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT (where applicable)**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % change**	**Comments (inc reasons for change in charges and/or income)**
	Housing - M. Davis - P Whitfield - Cllr Beresford							
251	Garages	Standard garages to Council tenants	N	£11.10	£11.22	**£184,950**	1.1%	Inflation increase 317 garages
252	Garages	Standard garages to Non-Council tenants	N	£11.10	£11.22	**£230,945**	1.1%	Inflation increase 475 garages
253	Garages	Garage Plots (per annum)	N	£132.93	£134.28	**£21,350**	1.0%	Inflation increase 159 garages
254	Garages let at full market rent	The Gateway, Dover	N	£19.22	£19.44	**£1,685**	1.1%	Inflation increase Two garages
255	Garages let at full market rent	Dover Town Area (Harold St, Godwyne Close, Pencester)	N	£17.22	£17.22	**£15,222**	0.0%	17 garages
256	Guest Room Rental	Rental of Guest Room in Sheltered Housing Blocks	N	£18.50	£18.50	£1,400	0.0%	£18.50 for the first night then £11.50 for any subsequent nights
257	Rent of Common Rooms	Rental of Common Rooms in Sheltered Housing Blocks	N	£10.00	£10.00	£1,500	0.0%	£10 per hour
258	Laundry Facilities	Use of Laundry Facilities within the Sheltered Housing Blocks	N	£0.20	£0.20	£600	0.0%	3000
259	Keys	Assa Keys for Communal Buildings	N	£18.00	£18.00	£900	0.0%	60
260	Supporting People Charges	Accommodation based service - sheltered	N	£10.24	£10.24	£142,021	0.0%	266 clients
261	Supporting People Charges	Alarm Service	N	£0.33	£0.33	£11,154	0.0%	650 clients (charge is per week)
262	Leaseholders	Solicitors enquiries from potential leaseholders	N	£108	£109.20	£3,185	1.1%	Inflation increase 35 expected
263	Notice of Transfer	Change of Leaseholder details		£75	£76.00	£2,280	1.3%	Inflation increase 30 expected
264	Leaseholders	Extension of Lease - initial work on lease valuation extension and legal costs. Does not include costs of actual lease extension		£656	£656	656	0.0%	One lease extension expected
265	Retrospective Consent	Retrospective consent from Housing to make alterations at Council Properties		£40	£45	£450	12.5%	More accurate reflection of actual cost 10 expected
	Private Sector Housing - M. Davis - R. Kennedy - Cllr Beresford							
266	HMO Licensing	Initial application fee to licence an HMO.	N	£680	£700	£1,600	2.9%	Change due to benchmarking of surrounding councils charges
267	HMO Licensing	Fee for Licence renewal	N	£450	£460	£1,800	2.2%	Change due to benchmarking of surrounding councils charges
268	Housing Act Notices	Improvement and Prohibition notice	N	£350	£370	£1,000	5.7%	Change due to benchmarking of surrounding councils charges

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT (where applicable)**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % change**	**Comments (inc reasons for change in charges and/or income)**
	Housing - M. Davis - P Whitfield - Cllr Beresford							
269	Housing Act Notices	Suspended Improvement and Prohibition notice	N	£350	£370	£0	5.7%	Change due to benchmarking of surrounding councils charges
270	Housing Act Notices	Emergency Remedial Action	N	£500	£550	£550	10.0%	Change due to benchmarking of surrounding councils charges
271	Housing Act Notices	Demolition Order	N	£600	£610	£0	1.7%	Inflation costs
272	Mobile Homes Act 2013 licence	Initial Licence fee	N	£50	£50	£0	0.0%	
273	Mobile Homes Act 2013 licence	Annual licence fee	N	£10	£10	£0	0.0%	For each pitch
274	Mobile Homes Act 2013 licence	Transfer of licence	N	£300	£300	£0	0.0%	For each licence
275	Mobile Homes Act 2013 licence	Expansion fee	N	£200	£200	£0	0.0%	For each expansion plus £10 for each additional unit
276	Mobile Homes Act 2013 licence	Fee for depositing rules	N	£30	£30	£0	0.0%	Depositing rules
277	Mobile Homes Act 2013 licence	Charge for notices	N	£260	£260	£0	0.0%	One notice plus cost for specialist reports
278	The redress schemes for letting agency work and management agency work order 2014	Penalty notice for each breach of requirement of lletting agent or managing agent to belong to a redress scheme	Y	£5,000	£5,000	£0	0.0%	Each breach of requirement
279	The Smoke and Carbon Monoxide Alarm (England) Regulations 2015	Penalty notice for each breach of requirement of lletting agent or managing agent to belong to a redress scheme	Max yes	£1,500	£1,500	£0	0.0%	£1500 for first offence; £3000 for second offence; £5000 for third and subsequent offence
280	Immigration inspection	Requests to inspect properties and provide report of suitability of property for immigration	N	£100	£100	0	0.0%	For one property inspection
	Miscellaneous - M. Davis - H. Lamb - Cllr Conolly							
281	Finance	Credit Card Surcharge	N		£0	**£0**	-100.0%	Credit card surcharge to be removed to encourage move to electronic payments and to support digital transformation.
282	Finance	Court Summons for Council Tax and Business Rates	N	£50	£50	£300,000	0.0%	No increase for 17/18 As the costs are only intended to reflect our actual costs in obtaining the summons or liability order it is difficult to justify increasing them when our overall budgets are reducing.
283	Finance	Liability Order for Council Tax and Business Rates	N	£50	£50		0.0%	

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % Change**	**Comments (inc reasons for change in charges and/or income)**
	Licensing - D. Randall - D. Croucher - Cllr Collor							
1	Personal Licences	Grant or Renewal	Y	£37	£37	**£3,700**	0%	Statutory Fee set by Government
2	Personal Licences	Change of Name or Address	Y	£10.50	£10.50	£315.00	0%	
3	Personal Licences	Theft, Loss etc.	Y	£10.50	£10.50	£52.50	0%	
4	Premises & Club Licences	Theft, Loss etc.	Y	£10.50	£10.50	£52.50	0%	
5	Premises & Club Licences	Change of Name or Address	Y	£10.50	£10.50	£52.50	0%	
6	Premises & Club Licences	Change of Club Rules	Y	£10.50	£10.50	£0	0%	
7	Premises & Club Licences	Vary DPS	Y	£23	£23	£1,886	0%	
8	Premises & Club Licences	Transfer Licence	Y	£23	£23	£621	0%	
9	Premises & Club Licences	Interim Authority	Y	£23	£23	£0	0%	
10	Premises & Club Licences	Notification Interest	Y	£21	£21	£21	0%	
11	Premises & Club Licences	Provisional Statement	Y	£315	£315	£0	0%	
12	Premises & Club Licences	Minor Variation	Y	£89	£89	£267	0%	
13	Premises & Club Licences	New Application & Variation NDR Band A	Y	£100	£100	£1,000	0%	
14	Premises & Club Licences	New Application & Variation NDR Band B	Y	£190	£190	£2,090	0%	

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % Change**	**Comments (inc reasons for change in charges and/or income)**
15	Premises & Club Licences	New Application & Variation NDR Band C	Y	£315	£315	£630	0%	
16	Premises & Club Licences	New Application & Variation NDR Band D	Y	£450	£450	£0	0%	
17	Premises & Club Licences	New Application & Variation NDR Band E	Y	£635	£635	£0	0%	
18	Premises & Club Licences	Annual Fee NDR Band A	Y	£70	£70	**£6,300**	0%	
19	Premises & Club Licences	Annual Fee NDR Band B	Y	£180	£180	**£54,000**	0%	
20	Premises & Club Licences	Annual Fee NDR Band C	Y	£295	£295	**£12,390**	0%	
21	Premises & Club Licences	Annual Fee NDR Band D	Y	£320	£320	**£3,520**	0%	
22	Premises & Club Licences	Annual Fee NDR Band E	Y	£350	£350	**£2,800**	0%	
23	Large Scale Events	New Application & Variation. Number in Attendance at any one time: 5,000 to 9,999	Y	£1,000	£1,000	£0	0%	
24	Large Scale Events	New Application & Variation. Number in Attendance at any one time: 10,000 to 14,999	Y	£2,000	£2,000	£0	0%	
25	Large Scale Events	New Application & Variation. Number in Attendance at any one time: 15,000 to 19,999	Y	£4,000	£4,000	£0	0%	
26	Large Scale Events	New Application & Variation. Number in Attendance at any one time: 20,000 to 29,999	Y	£8,000	£8,000	£0	0%	

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % Change**	**Comments (inc reasons for change in charges and/or income)**
27	Large Scale Events	New Application & Variation. Number in Attendance at any one time: 30,000 to 39,999	Y	£16,000	£16,000	£0	0%	Statutory Fee set by Government
28	Large Scale Events	New Application & Variation. Number in Attendance at any one time: 40,000 to 49,999	Y	£24,000	£24,000	£0	0%	
29	Large Scale Events	New Application & Variation. Number in Attendance at any one time: 50,000 to 59,999	Y	£32,000	£32,000	£0	0%	
30	Large Scale Events	New Application & Variation. Number in Attendance at any one time: 60,000 to 69,999	Y	£40,000	£40,000	£0	0%	
31	Large Scale Events	New Application & Variation. Number in Attendance at any one time: 70,000 to 79,999	Y	£48,000	£48,000	£0	0%	
32	Large Scale Events	New Application & Variation. Number in Attendance at any one time: 80,000 to 89,999	Y	£56,000	£56,000	£0	0%	
33	Large Scale Events	New Application & Variation. Number in Attendance at any one time: 90,000 and over	Y	£64,000	£64,000	£0	0%	
34	Large Scale Events	Annual Fee 5,000 to 9,999	Y	£500	£500	£0	0%	
35	Large Scale Events	Annual Fee 10,000 to 14,999	Y	£1,000	£1,000	£0	0%	
36	Large Scale Events	Annual Fee 15,000 to 19,999	Y	£2,000	£2,000	£0	0%	
37	Large Scale Events	Annual Fee 20,000 to 29,999	Y	£4,000	£4,000	£0	0%	
38	Large Scale Events	Annual Fee 30,000 to 39,999	Y	£8,000	£8,000	£0	0%	

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % Change**	**Comments (inc reasons for change in charges and/or income)**
39	Large Scale Events	Annual Fee 40,000 to 49,999	Y	£12,000	£12,000	£0	0%	
40	Large Scale Events	Annual Fee 50,000 to 59,999	Y	£16,000	£16,000	£0	0%	
41	Large Scale Events	Annual Fee 60,000 to 69,999	Y	£20,000	£20,000	£0	0%	Statutory Fee set by Government
42	Large Scale Events	Annual Fee 70,000 to 79,999	Y	£24,000	£24,000	£0	0%	
43	Large Scale Events	Annual Fee 80,000 to 89,999	Y	£28,000	£28,000	£0	0%	
44	Large Scale Events	Annual fee 90,000 and over	Y	£32,000	£32,000	£0	0%	
45	Temporary Event Notices	New Notice	Y	£21	£21	£4,830	0%	
46	Temporary Event Notices	Theft, Loss etc.	Y	£10.50	£10.50	£0.00	0%	
47	Small Society Lotteries	Registration Fee	Y	£40	£40	£480	0%	
48	Small Society Lotteries	Annual Fee	Y	£20	£20	£1,400	0%	

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income inc VAT**	**Fee % Change**	**Comments (inc reasons for change in charges and/or income)**
	Licensing - D. Randall - D. Croucher - Cllr Collor							
49	Bingo Club	Licence Application	N	£3,500	£3,500	£0	0%	
50	Bingo Club	Annual Fee	N	£950	£950	£1,900	0%	
51	Bingo Club	Application to Vary	N	£1,750	£1,750	£0	0%	
52	Bingo Club	Application to Transfer	N	£1,200	£1,200	£0	0%	
53	Bingo Club	Application for Reinstatement	N	£1,200	£1,200	£0	0%	
54	Bingo Club	Application for Provisional Statement	N	£3,500	£3,500	£0	0%	
55	Bingo Club	Licence Application (Provisional Statement Holders)	N	£1,200	£1,200	£0	0%	
56	Bingo Club	Copy of Licence	N	£25	£25	£0	0%	
57	Bingo Club	Notification of Change	N	£50	£50	£0	0%	
58	Betting Premise (excluding Tracks)	Licence Application	N	£3,000	£3,000	£0	0%	
59	Betting Premise (excluding Tracks)	Annual Fee	N	£575	£575	£6,325	0%	
60	Betting Premise (excluding Tracks)	Application to Vary	N	£1,250	£1,250	£0	0%	
61	Betting Premise (excluding Tracks)	Application to Transfer	N	£1,200	£1,200	£0	0%	
62	Betting Premise (excluding Tracks)	Application for Reinstatement	N	£1,200	£1,200	£0	0%	
63	Betting Premise (excluding Tracks)	Application for Provisional Statement	N	£3,000	£3,000	£0	0%	
64	Betting Premise (excluding Tracks)	Licence Application (Provisional Statement Holders)	N	£1,200	£1,200	£0	0%	
65	Betting Premise (excluding Tracks)	Copy of Licence	N	£25	£25	£0	0%	

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income inc VAT**	**Fee % Change**	**Comments (inc reasons for change in charges and/or income)**
66	Betting Premise (excluding Tracks)	Notification of Change	N	£50	£50	£0	0%	
67	Track	Licence Application	N	£2,500	£2,500	£0	0%	
68	Track	Annual Fee	N	£950	£950	£0	0%	
69	Track	Application to Vary	N	£1,250	£1,250	£0	0%	
70	Track	Application to Transfer	N	£950	£950	£0	0%	
71	Track	Application for Reinstatement	N	£950	£950	£0	0%	
72	Track	Application for Provisional Statement	N	£2,500	£2,500	£0	0%	
73	Track	Licence Application (Provisional Statement Holders)	N	£950	£950	£0	0%	
74	Track	Copy of Licence	N	£25	£25	£0	0%	
75	Track	Notification of Change	N	£50	£50	£0	0%	
76	Family Entertainment Centre	Licence Application	N	£2,000	£2,000	£0	0%	
77	Family Entertainment Centre	Annual Fee	N	£725	£725	£2,175	0%	
78	Family Entertainment Centre	Application to Vary	N	£1,000	£1,000	£0	0%	
79	Family Entertainment Centre	Application to Transfer	N	£950	£950	£0	0%	
80	Family Entertainment Centre	Application for Reinstatement	N	£950	£950	£0	0%	
81	Family Entertainment Centre	Application for Provisional Statement	N	£2,000	£2,000	£0	0%	
82	Family Entertainment Centre	Licence Application (Provisional Statement Holders)	N	£950	£950	£0	0%	
83	Family Entertainment Centre	Copy of Licence	N	£25	£25	£0	0%	
84	Family Entertainment Centre	Notification of Change	N	£50	£50	£0	0%	

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income inc VAT**	**Fee % Change**	**Comments (inc reasons for change in charges and/or income)**
85	Adult Gaming Centre	Licence Application	N	£2,000	£2,000	£0	0%	
86	Adult Gaming Centre	Annual Fee	N	£950	£950	**£3,800**	0%	
87	Adult Gaming Centre	Application to Vary	N	£1,000	£1,000	£0	0%	
88	Adult Gaming Centre	Application to Transfer	N	£1,200	£1,200	£0	0%	
89	Adult Gaming Centre	Application for Reinstatement	N	£1,200	£1,200	£0	0%	
90	Adult Gaming Centre	Application for Provisional Statement	N	£2,000	£2,000	£0	0%	
91	Adult Gaming Centre	Licence Application (Provisional Statement Holders)	N	£1,200	£1,200	£0	0%	
92	Adult Gaming Centre	Copy of Licence	N	£25	£25	£0	0%	
93	Adult Gaming Centre	Notification of Change	N	£50	£50	£0	0%	
94	New Small Casino	Licence Application	N	£8,000	£8,000	£0	0%	
95	New Small Casino	Annual Fee	N	£5,000	£5,000	£0	0%	
96	New Small Casino	Application to Vary	N	£4,000	£4,000	£0	0%	
97	New Small Casino	Application to Transfer	N	£1,800	£1,800	£0	0%	
98	New Small Casino	Application for Reinstatement	N	£1,800	£1,800	£0	0%	
99	New Small Casino	Application for Provisional Statement	N	£8,000	£8,000	£0	0%	
100	New Small Casino	Licence Application (Provisional Statement Holders)	N	£3,000	£3,000	£0	0%	
101	New Small Casino	Copy of Licence	N	£25	£25	£0	0%	
102	New Small Casino	Notification of Change	N	£50	£50	£0	0%	
103	New Large Casino	Licence Application	N	£10,000	£10,000	£0	0%	
104	New Large Casino	Annual Fee	N	£10,000	£10,000	£0	0%	

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income inc VAT**	**Fee % Change**	**Comments (inc reasons for change in charges and/or income)**
105	New Large Casino	Application to Vary	N	£5,000	£5,000	£0	0%	
106	New Large Casino	Application to Transfer	N	£2,150	£2,150	£0	0%	
107	New Large Casino	Application for Reinstatement	N	£2,150	£2,150	£0	0%	
108	New Large Casino	Application for Provisional Statement	N	£10,000	£10,000	£0	0%	
109	New Large Casino	Licence Application (Provisional Statement Holders)	N	£5,000	£5,000	£0	0%	
110	New Large Casino	Copy of Licence	N	£25	£25	£0	0%	
111	New Large Casino	Notification of Change	N	£50	£50	£0	0%	
112	Regional Casino	Licence Application	N	£15,000	£15,000	£0	0%	
113	Regional Casino	Annual Fee	N	£15,000	£15,000	£0	0%	
114	Regional Casino	Application to Vary	N	£7,500	£7,500	£0	0%	
115	Regional Casino	Application to Transfer	N	£6,500	£6,500	£0	0%	
116	Regional Casino	Application for Reinstatement	N	£6,500	£6,500	£0	0%	
117	Regional Casino	Application for Provisional Statement	N	£15,000	£15,000	£0	0%	
118	Regional Casino	Licence Application (Provisional Statement Holders)	N	£8,000	£8,000	£0	0%	
119	Regional Casino	Copy of Licence	N	£25	£25	£0	0%	
120	Regional Casino	Notification of Change	N	£50	£50	£0	0%	
121	Temporary Use Notice	Application Fee	Y	£500	£500	£0	0%	
122	Alcohol Licences Premises	Permit Application Fee (2 or less Machines)	Y	£50	£50	£250	0%	

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income inc VAT**	**Fee % Change**	**Comments (inc reasons for change in charges and/or income)**
123	Alcohol Licences Premises	Permit Application Fee (3+ Machines)	Y	£150	£150	£0	0%	
124	Alcohol Licences Premises	Permit Annual Fee (3+ Machines)	Y	£50	£50	£150	0%	
125	Family Entertainment Centre Unlicensed	Permit Application Fee	Y	£300	£300	£0	0%	
126	Family Entertainment Centre Unlicensed	Permit Renewal Fee	Y	£300	£300	**£1,800**	0%	Permits last for a period of 10 years.
127	Prize Gaming	Permit Application Fee	Y	£300	£300	£0	0%	
128	Prize Gaming	Permit Renewal Fee	Y	£300	£300	£0	0%	
129	Club Gaming	Permit Application Fee	Y	£200	£200	£0	0%	
130	Club Gaming	Permit Annual Fee	Y	£50	£50	£100	0%	
131	Club Gaming	Permit Renewal Fee (due every 10 years)	Y	£200	£200	£0	0%	
132	Club Gaming Machine	Permit Application Fee	Y	£200	£200	£0	0%	
133	Club Gaming Machine	Permit Annual Fee	Y	£50	£50	£250	0%	
134	Club Gaming Machine	Permit Renewal Fee	Y	£200	£200	£0	0%	
135	Club Fast-track for Gaming Permit or Gaming Machine Permit	Permit Application Fee	Y	£100	£100	£0	0%	

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income inc VAT**	**Fee % Change**	**Comments (inc reasons for change in charges and/or income)**
136	Club Fast-track for Gaming Permit or Gaming Machine Permit	Permit Annual Fee	Y	£50	£50	£0	0%	
137	Gaming Machine Permit	Annual Fee	Y	£100	£100	£0	0%	
138	Provision of Gambling	Copy Licence	Y	£0	£0	£0	0%	
139	Provision of Gambling	Notification of Change	Y	£0	£0	£0	0%	

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % Change**	**Comments (inc reasons for change in charges and/or income)**
	Licensing - D. Randall - D. Croucher - Cllr Collor							
1	Acupuncture	Premise Registration	N	£175	£175	£0	0%	
2	Acupuncture	Additional Practitioner	N	£80	£80	£80	0%	
3	Acupuncture	Minor Variation	N	£50	£50	£0	0%	
4	Cosmetic Piercing	Premise Registration	N	£175	£175	£0	0%	
5	Cosmetic Piercing	Additional Practitioner	N	£80	£80	£80	0%	
6	Cosmetic Piercing	Minor Variation	N	£50	£50	£0	0%	
7	Ear Piercing	Premise Registration	N	£175	£175	£0	0%	
8	Ear Piercing	Additional Practitioner	N	£80	£80	£80	0%	
9	Ear Piercing	Minor Variation	N	£50	£50	£0	0%	
10	Electrolysis	Premise Registration	N	£175	£175	£0	0%	
11	Electrolysis	Additional Practitioner	N	£80	£80	£0	0%	
12	Electrolysis	Minor Variation	N	£50	£50	£0	0%	
13	Semi-permanent Skin-colouring	Premise Registration	N	£175	£175	£0	0%	
14	Semi-permanent Skin-colouring	Additional Practitioner	N	£80	£80	£80	0%	
15	Semi-permanent Skin-colouring	Minor Variation	N	£50	£50	£0	0%	
16	Tattooing	Premise Registration	N	£175	£175	£0	0%	
17	Tattooing	Additional Practitioner	N	£80	£80	£80	0%	

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % Change**	**Comments (inc reasons for change in charges and/or income)**
18	Tattooing	Minor Variation	N	£50	£50	£0	0%	
19	Animal Licensing	Boarding Establishments	N	£235	£235	**£3,290**	0%	Plus vet fees (initial visit). NOTE: £157 Non refundable to be submitted with application, a further £78 is due if application is approved to cover regulation.
20	Animal Licensing	Home Boarding	N	£120	£120	**£480**		Boarding within Domestic Premises. Plus vet fees (initial visit). NOTE: £80 Non refundable to be submitted with application, a further £40 is due if application is approved to cover regulation.
21	Animal Licensing	Dog Breeding Establishments	N	£235	£235	£470	0%	Plus Vet fees. NOTE: £157 Non refundable to be submitted with application, a further £78 is due if application is approved to cover regulation.
22	Animal Licensing	Dangerous Wild Animals	N	£235	£235	£0	0%	Every 2 years Plus Vet fees. NOTE: £157 Non refundable to be submitted with application, a further £78 is due if application is approved to cover regulation.
23	Animal Licensing	Performing Animals	N	£235	£235	£0	0%	Plus Vet fees. NOTE: £157 Non refundable to be submitted with application, a further £78 is due if application is approved to cover regulation.

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % Change**	**Comments (inc reasons for change in charges and/or income)**
24	Animal Licensing	Pet Shops	N	£170	£170	£1,020	0%	Plus vet fees (initial visit). Plus vet fees (initial visit). NOTE: £114 Non refundable to be submitted with application, a further £56 is due if application is approved to cover regulation.
25	Animal Licensing	Horse Riding Establishments	N	£235	£235	£940	0%	Plus Vet fees. NOTE: £157 Non refundable to be submitted with application, a further £78 is due if application is approved to cover regulation.
26	Animal Licensing	Zoos	N	£750	£750	£0	0%	Every 4-6 years (Plus interim vet inspection fees during period) Plus Vet fees. NOTE: £500 Non refundable to be submitted with application, a further £250 is due if application is approved to cover regulation.
27	Street Trading Consent	Grant	N	£490	£490	£490	0%	£295 Non refundable to be submitted with application, a further £195 is due if application is approved to cover regulation.
28	Street Trading Consent	Annual renewal	N	£230	£230	£920	0%	
29	Street Trading Consent	Occasional	N	£130	£130	£0	0%	
30	Street Trading Consent	Occasional Street Market	N	£200	£200	£1,000	0%	Up to 25 stalls then £10 per stall thereafter

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % Change**	**Comments (inc reasons for change in charges and/or income)**
31	Street Trading Consent	Pavement Permit (New) - Tables & Chairs	N	£75	£75	£150	0%	New & Variation Applications
32	Street Trading Consent	Pavement Permit (Renewal) - Tables & Chairs	N	£35	£35	£980	0%	Renewal
33	Sexual Entertainment Venue	Grant	N	£3,250	£3,250	£0	0%	NOTE: £2167 Non refundable to be submitted with application, a further £1083 is due if application is approved to cover regulation.
34	Sexual Entertainment Venue	Renewal, Transfer or Variation	N	£2,225	£2,225	£0	0%	NOTE: £1484 Non refundable to be submitted with application, a further £741 is due if application is approved to cover regulation.
35	Boat Licence	Grant	N	£93	£93	£0	0%	
36	Boat Licence	Renewal or Transfer	N	£93	£93	£279	0%	
37	Hypnotism Performance	Grant	N	£50	£50	£0	0%	
38	Scrap Metal Dealer	Site Licence Grant	N	£470	£470	£0	0%	NOTE: £314 Non refundable to be submitted with application, a further £156 is due if application is approved to cover regulation.
39	Scrap Metal Dealer	Site Licence Variation	N	£50	£50	£0	0%	
40	Scrap Metal Dealer	Site Licence Renewal	N	£450	£450	**£0**	0%	Every 3 years

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**Fee % Change**	**Comments (inc reasons for change in charges and/or income)**
41	Scrap Metal Dealer	Collectors Licence Grant	N	£275	£275	£0	0%	NOTE: £184 Non refundable to be submitted with application, a further £91 is due if application is approved to cover regulation.
42	Scrap Metal Dealer	Collectors Licence Variation	N	£50	£50	£0	0%	
43	Scrap Metal Dealer	Collectors Licence Renewal	N	£255	£255	£255	0%	Every 3 years

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**% Change**	**Comments (inc reasons for change in charges and/or income)**
	Licensing - D. Randall - D. Croucher - Cllr Collor							
44	Hackney Carriage & Private Hire	Hackney Carriage Vehicle Annual Licence (Grant and Renewal)	N	£375	£327	**£22,080**	-13%	If vehicle is wheelchair accessible there is a 10% reduction in fee
45	Hackney Carriage & Private Hire	Private Hire Vehicle Annual Licence (Grant and Renewal)	N	£315	£259	**£33,012**	-18%	No part of this fee is refundable in the event that the application is not approved or the vehicle is delicensed for any reason during the licence period. If vehicle is wheelchair accessible there is a 10% reduction in fee.
46	Hackney Carriage & Private Hire	Unmet Demand Survey	N	£0	£0	£0		Included within Grant / renewal Fee
47	Hackney Carriage & Private Hire	Licence Transfer Following Change of Vehicle	N	£50	£54	£2,800	8%	
48	Hackney Carriage & Private Hire	Change of Vehicle ownership	N	£20	£21	£42	5%	
49	Hackney Carriage & Private Hire	Joint Hackney Carriage Private Hire Driver: 1 year (Grant)	N	£91	£124.00		37%	No part of this fee is refundable in the event that the application is not approved or the driver is delicensed for any reason during the Licence period.
50	Hackney Carriage & Private Hire	Joint Hackney Carriage Private Hire Driver: 1 year (Renewal)	N		£110.00			No part of this fee is refundable in the event that the application is not approved or the driver is delicensed for any reason during the Licence period.

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**% Change**	**Comments (inc reasons for change in charges and/or income)**
	Licensing - D. Randall - D. Croucher - Cllr Collor							
51	Hackney Carriage & Private Hire	Joint Hackney Carriage Private Hire Driver: 3 year (Grant)	N	£187	£293.00	**£30,000**	N/A	The first year (£124) is non refundable in the event that the application is not approved or the driver is delicensed for any reason during the Licence period. Any further refunds will be dealt with on a case by case basis.
52	Hackney Carriage & Private Hire	Joint Hackney Carriage Private Hire Driver: 3 year (Renewal)	N		£279.00			The first year (£110) is non refundable in the event that the application is not approved or the driver is delicensed for any reason during the Licence period. Any further refunds will be dealt with on a case by case basis.
53	Hackney Carriage & Private Hire	DBS Disclosure (formerly CRB)	N	£44	£44	**£5,060**	0%	Fee set externally. New drivers + every 3 years for renewals
54	Hackney Carriage & Private Hire	Knowledge Test	N	£26	£0	£0	-100%	Included within Grant fee
55	Hackney Carriage & Private Hire	Vehicle Plate	N	£19	£17	£306	-11%	Per plate
56	Hackney Carriage & Private Hire	Vehicle Plate holder	N	£12	£15	£150	25%	Per holder

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**% Change**	**Comments (inc reasons for change in charges and/or income)**
	Licensing - D. Randall - D. Croucher - Cllr Collor							
57	Private Hire Operator	Operators Licence for PH Vehicles Only (not Hackney) (1 year Licence) 1 to 5 vehicles	N	£15 Plus £40 per vehicle	£90		0%	1 year licence only available in exceptional circumstances. No part of this fee is refundable in any the event.
58	Private Hire Operator	Operators Licence for PH Vehicles Only (not Hackney) (1 year Licence) 6 to 10 vehicles	N		£144			1 year licence only available in exceptional circumstances. No part of this fee is refundable in any the event.
59	Private Hire Operator	Operators Licence for PH Vehicles Only (not Hackney) (1 year Licence) Over 10 vehicles	N		£197			1 year licence only available in exceptional circumstances. No part of this fee is refundable in any the event.

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**% Change**	**Comments (inc reasons for change in charges and/or income)**
	Licensing - D. Randall - D. Croucher - Cllr Collor							
60	Private Hire Operator	Operators Licence for PH Vehicles Only (not Hackney) (Licence lasts 5 years) 1 to 5 vehicles	N	£75 Plus £200 per vehicle	£364	£2,480	N/A	Licence lasts 5 years. The first year (£90) is non refundable in any event. Refunds will be considered in subsequent years if the licenced is surrendered or revoked during the period of the licence.
61	Private Hire Operator	Operators Licence for PH Vehicles Only (not Hackney) (Licence lasts 5 years) 6 to 10 vehicles	N		£631			Licence lasts 5 years. The first year (£144) is non refundable in any event. Refunds will be considered in subsequent years if the licenced is surrendered or revoked during the period of the licence.

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT (where applicable)**	**Total Expected Income ex VAT**	**% Change**	**Comments (inc reasons for change in charges and/or income)**
	Licensing - D. Randall - D. Croucher - Cllr Collor							
62	Private Hire Operator	Operators Licence for PH Vehicles Only (not Hackney) (Licence lasts 5 years) 11 or more vehicles	N		£898			Licence lasts 5 years. The first year (£197) is non refundable in any event. Refunds will be considered in subsequent years if the licenced is surrendered or revoked during the period of the licence.
63	Private Hire Operator	Variation to Operators Licence (within band) for PH Vehicles	N		£30	£200.00		New fee to allow for changes such as change of name or number of vehicles.
64	Private Hire Operator	Variation to Operators Licence (outside of band) for PH Vehicles	N		£50			New fee to allow for changes such as change of name or number of vehicles.

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT**	**Total Expected Income ex VAT**	**Fee % change**	**Reasons for Change in Charges and/or income**
	Planning - N. Aziz - M. Ebbs - Cllr Kenton							
1	General	Section 52 Agreements, Section 106 Agreements, Tree Preservation Orders and Article 4 Directions and Enforcement Notices	Y	£5.00	£5.00			
2	General	Plans submitted with planning applications or accompanying other planning documents and other miscellaneous photocopying	N	£0.10	£0.10			A4
3	General	Plans submitted with planning applications or accompanying other planning documents and other miscellaneous photocopying	N	£0.20	£0.20	£750.00		A3
4	General	Plans submitted with planning applications or accompanying other planning documents and other miscellaneous photocopying	N	£5.00	£5.00			Over A3
5	General	Research on Planning Histories, Permitted Development Rights and Use classes	N	£35.00	£35.00			Per request
6	General	Planning Application Fees (see Appendix 5.2 - A Guide to the Fees for Planning Applications in England)	Y			**£600,000**	9%	Increase projected based on i) the current fees received to date this financial year and ii) possible fee increases proposed by the Govt
7	General	Pre-application advice (see Appendix 5.3)	N			**£55,000**	0%	

				2016/17	2017/18	2017/18		
	Detail	**Narrative**	**Set by Government? Y/N**	**Approved Charges inc VAT**	**Proposed Charges inc VAT**	**Total Expected Income ex VAT**	**Fee % change**	**Reasons for Change in Charges and/or income**
	Planning - N. Aziz - M. Ebbs - Cllr Kenton							
8	General	Details pursuant to conditions	Y				0%	
9	General	Details pursuant to conditions	Y				0%	
10	General	Advice on compliance of conditions information	Y			**£15,000**	0%`	
11	General	Advice on compliance of conditions information	Y				0%	

A Guide to the Fees for Planning Applications in England

These fees apply from 15 April 2015 onwards.

This document is based upon '*The Town and Country Planning (Fees for Applications, Deemed Applications, Requests and Site Visits) (England) Regulations 2012*'

The fee should be paid at the time the application is submitted. If you are unsure of the fee applicable, please contact your Local Planning Authority.

All Outline Applications		
£385 per 0.1 hectare for sites up to and including 2.5 hectares	Not more than 2.5 hectares	£385 per 0.1 hectare
£9,527 + £115 for each 0.1 in excess of 2.5 hectares to a maximum of £125,000	More than 2.5 hectares	£9,527 + £115 per 0.1 hectare

Householder Applications		
Alterations/extensions to a **single dwelling,** including works within boundary	Single dwelling	£172

Full Applications (and First Submissions of Reserved Matters)		
Alterations/extensions to **two or more dwellings**, including works within boundaries	Two or more dwellings (or two or more flats)	£339
New dwellings (up to and including 50)	New dwellings (not more than 50)	£385 per dwelling
New dwellings (for *more* than 50) £19,049 + £115 per additional dwelling in excess of 50 up to a maximum fee of £250,000	New dwellings (more than 50)	£19,049 + £115 per additional dwelling

Continued on next page…

Full Applications (and First Submissions of Reserved Matters) continued…		
Erection of buildings (not dwellings, agricultural, glasshouses, plant nor machinery):		
Gross floor space to be created by the development	No increase in gross floor space or no more than 40 sq m	£195
Gross floor space to be created by the development	More than 40 sq m but no more than 75 sq m	£385
Gross floor space to be created by the development	More than 75 sq m but no more than 3,750 sq m	£385 for each 75sq m or part thereof
Gross floor space to be created by the development	More than 3,750 sq m	£19,049 + £115 for each additional 75 sq m in excess of 3750 sq m to a maximum of £250,000
The erection of buildings (on land used for agriculture for agricultural purposes)		
Gross floor space to be created by the development	Not more than 465 sq m	£80
Gross floor space to be created by the development	More than 465 sq m but not more than 540 sq m	£385
Gross floor space to be created by the development	More than 540 sq m but not more than 4,215 sq m	£385 for first 540 sq m + £385 for each 75 sq m (or part thereof) in excess of 540 sq m
Gross floor space to be created by the development	More than 4,215 sq m	£19,049 + £115 for each 75 sq m (or part thereof) in excess of 4,215 sq m up to a maximum of £250,000

Continued on next page…

Full Applications (and First Submissions of Reserved Matters) continued…		
Erection of glasshouses (on land used for the purposes of agriculture)		
Gross floor space to be created by the development	Not more than 465 sq m	£80
Gross floor space to be created by the development	More than 465 sq m	£2,150
Erection / alterations / replacement of plant and machinery		
Site area	Not more than 5 hectares	£385 for each 0.1 hectare (or part thereof)
Site area	More than 5 hectares	£19,049 + additional £115 for each 0.1 hectare (or part thereof) in excess of 5 hectares to a maximum of £250,000

Applications other than Building Works		
Car parks, service roads or other accesses	For existing uses	£195
Waste (Use of land for disposal of refuse or waste materials or deposit of material remaining after extraction or storage of minerals)		
Site area	Not more than 15 hectares	£195 for each 0.1 hectare (or part thereof)
Site area	More than 15 hectares	£29,112 + £115 for each 0.1 hectare (or part thereof) in excess of 15 hectares up to a maximum of £65,000
Operations connected with exploratory drilling for oil or natural gas		
Site area	Not more than 7.5 hectares	£423 for each 0.1 hectare (or part thereof)
Site area	More than 7.5 hectares	£31,725 + additional £126 for each 0.1 hectare (or part thereof) in excess of 7.5 hectares up to a maximum of £250,000

Continued on next page…

Operations (other than exploratory drilling) for the winning and working of oil or natural gas		
Site area	Not more than 15 hectares	£214 for each 0.1 hectare (or part thereof)
Site area	More than 15 hectares	£32,100 + additional £126 for each 0.1 in excess of 15 hectare up to a maximum of £65,000
Other operations (winning and working of minerals) excluding oil and natural gas		
Site area	Not more than 15 hectares	£195 for each 0.1 hectare (or part thereof)
Site area	More than 15 hectares	£29,112 + additional £115 for each 0.1 in excess of 15 hectare up to a maximum of £65,000
Other operations (not coming within any of the above categories)		
Site area	Any site area	£195 for each 0.1 hectare (or part thereof) up to a maximum of £1,690

Lawful Development Certificate	
Existing use or operation	Same as Full
Existing use or operation - lawful not to comply with any condition or limitation	£195
Proposed use or operation	Half the normal planning fee.

Continued on next page…

Prior Approval	
Agricultural and Forestry buildings & operations or demolition of buildings	£80
Telecommunications Code Systems Operators	£385
Proposed Change of Use to State Funded School or Registered Nursery	£80
Proposed Change of Use of Agricultural Building to a State-Funded School or Registered Nursery	£80
Proposed Change of Use of Agricultural Building to a flexible use within Shops, Financial and Professional services, Restaurants and Cafes, Business, Storage or Distribution, Hotels, or Assembly or Leisure	£80
Proposed Change of Use of a building from Office (Use Class B1) Use to a use falling within Use Class C3 (Dwellinghouse)	£80
Proposed Change of Use of Agricultural Building to a Dwellinghouse (Use Class C3), where there are no Associated Building Operations	£80
Proposed Change of Use of Agricultural Building to a Dwellinghouse (Use Class C3), and Associated Building Operations	£172
Proposed Change of Use of a building from a Retail (Use Class A1 or A2) Use or a Mixed Retail and Residential Use to a use falling within Use Class C3 (Dwellinghouse), where there are no Associated Building Operations	£80
Proposed Change of Use of a building from a Retail (Use Class A1 or A2) Use or a Mixed Retail and Residential Use to a use falling within Use Class C3 (Dwellinghouse), and Associated Building Operations	£172
Notification for Prior Approval for a Change Of Use from Storage or Distribution Buildings (Class B8) and any land within its curtilage to Dwellinghouses (Class C3)	£80
Notification for Prior Approval for a Change of Use from Amusement Arcades/Centres and Casinos, (Sui Generis Uses) and any land within its curtilage to Dwellinghouses (Class C3)	£80
Notification for Prior Approval for a Change of Use from Amusement Arcades/Centres and Casinos, (Sui Generis Uses) and any land within its curtilage to Dwellinghouses (Class C3), and Associated Building Operations	£172

Continued on next page…

Prior Approval continued…	
Notification for Prior Approval for a Change of Use from Shops (Class A1), Financial and Professional Services (Class A2), Betting Offices, Pay Day Loan Shops and Casinos (Sui Generis Uses) to Restaurants and Cafés (Class A3)	£80
Notification for Prior Approval for a Change of Use from Shops (Class A1), Financial and Professional Services (Class A2), Betting Offices, Pay Day Loan Shops and Casinos (Sui Generis Uses) to Restaurants and Cafés (Class A3), and Associated Building Operations	£172
Notification for Prior Approval for a Change of Use from Shops (Class A1) and Financial and Professional Services (Class A2), Betting Offices, Pay Day Loan Shops (Sui Generis Uses) to Assembly and Leisure Uses (Class D2)	£80

Reserved Matters	
Application for approval of reserved matters following outline approval	Full fee due or if full fee already paid then £385 due

Approval / Variation / discharge of condition	
Application for removal or variation of a condition following grant of planning permission	£195
Request for confirmation that one or more planning conditions have been complied with	£28 per request for Householder otherwise £97 per request

Change of Use of a building to use as one or more separate dwellinghouses, or other cases		
Number of dwellings	Not more than 50 dwellings	£385 for each
Number of dwellings	More than 50 dwellings	£19,049 + £115 for each in excess of 50 up to a maximum of £250,000
Other Changes of Use of a building or land		£385

Continued on next page…

Advertising	
Relating to the business on the premises	£110
Advance signs which are not situated on or visible from the site, directing the public to a business	£110
Other advertisements	£385

Application for a New Planning Permission to replace an Extant Planning Permission	
Applications in respect of major developments	£575
Applications in respect of householder developments	£57
Applications in respect of other developments	£195

Application for a Non-material Amendment Following a Grant of Planning Permission	
Applications in respect of householder developments	£28
Applications in respect of other developments	£195

Continued on next page…

CONCESSIONS
EXEMPTIONS FROM PAYMENT
For alterations, extensions, etc. to a dwelling house for the benefit of a registered disabled person
An application solely for the carrying out of the operations for the purpose of providing a means of access for disabled persons to or within a building or premises to which members of the public are admitted
Listed Building Consent
Planning permission for relevant demolition in a Conservation Area
Works to Trees covered by a Tree Preservation Order or in a Conservation Area Hedgerow Removal
If the proposal is the first revision of an application for development of the same character or description on the same site by the same applicant within 12 months of making the earlier application if withdrawn or the date of decision if granted or refused (including signs only if withdrawn or refused) and NOT a duplicate application made by the same applicant within 28 days
If the proposal relates to works that require planning permission only by virtue of an Article 4 Direction of the Town & Country Planning (General Permitted Development) Order 1995. I.e. where the application is required only because of a direction or planning condition removing permitted development rights.
If the application is for a lawful development certificate, for existing use, where an application for planning permission for the same development would be exempt from the need to pay a planning fee under any other planning fee regulation
If the application is for consent to display an advertisement following either a withdrawal of an earlier application (before notice of decision was issued) or where the application is made following refusal of consent for display of an advertisement, and where the application is made by or on behalf of the same person
If the application is for consent to display an advertisement which results from a direction under Regulation 7 of the 2007 Regulations, dis-applying deemed consent under Regulation 6 to the advertisement in question
If the application is for alternate proposals for the same site by the same applicant, in order to benefit from the permitted development right in Schedule 2 Part 3 Class E of the Town and Country Planning (General Permitted Development) Order 1995
If the application relates to a condition or conditions on an application for Listed Building Consent or planning permission for relevant demolition in a Conservation Area
If the application is for a Certificate of Lawfulness of Proposed Works to a listed building
Prior Approval for a Proposed Larger Home Extension

Continued on next page…

CONCESSIONS continued…
EXEMPTIONS FROM PAYMENTS continued…
Notification for Prior Approval for a Development Consisting of the Erection or Construction of a Collection Facility within the Curtilage of a Shop
Notification for Prior Approval for the Temporary Use of Buildings or Land for the Purpose of Commercial Film-Making and the Associated Temporary Structures, Works, Plant or Machinery required in Connection with that Use
Notification for Prior Approval for the Installation, Alteration or Replacement of other Solar Photovoltaics (PV) equipment on the Roofs of Non-domestic Buildings, up to a Capacity of 1 Megawatt

CONCESSIONS
REDUCTIONS TO PAYMENTS
If the application is being made on behalf of a non-profit making sports club for works for playing fields not involving buildings then the fee is £385
If the application is being made on behalf of a parish or community council then the fee is 50%
If the application is an alternative proposal being submitted on the same site by the same applicant on the same day, where this application is of lesser cost then the fee is 50%
In respect of reserved matters you must pay a sum equal to or greater than what would be payable at current rates for approval of all the reserved matters. If this amount has already been paid then the fee is £385
If the application is for a Lawful Development Certificate for a Proposed use or development, then the fee is 50%
If two or more applications are submitted for different proposals on the same day and relating to the same site then you must pay the fee for the highest fee plus half sum of the others
Where an application relates to development which is within more than one fee category, the correct fee is simply the highest of the fees payable (if not including residential)
Where an application consists of the erection of dwellings and the erection of other types of buildings (categories 1-4) the fees are added together and maximum can be exceeded
Where an application crosses one or more local or district planning authorities then the fee is 150% and goes to the authority that contains the larger part of the application site or a sum of the fees if it is less than 150%

ENDS

Pre-application Advice

Why Seek Advice?

Whether you are a developer of a large scheme or a householder wishing to improve your home, it is advisable to seek advice before submitting your planning application. We can let you know whether your proposals are supported by planning policy and whether there are any issues that may prevent you from obtaining planning permission.

Basic administrative advice on the planning process is available by visiting a local office or over the telephone and our website contains a wealth of information on planning matters. All of this is available free of charge.

If you would prefer a specific review of your proposals and detailed guidance on the application process, we would recommend you obtain formal pre-application advice. This is a charged-for service and is available to meet any scheme.

We are happy to provide advice at any time, whether it is just a discussion on some initial ideas or a review of more detailed plans. You can use the service just once or it is often beneficial to obtain advice throughout the evolution of your scheme.

There are considerable benefits in seeking our advice such as

- It gives you an opportunity to understand how our policies will be applied to your development
- It can identify at an early stage where there is a need for specialist input, for example about listed buildings, trees, landscape, noise, transport, contaminated land, ecology or archaeology
- It will assist you in preparing proposals for formal submission which, providing you have taken our advice fully into account, will be handled more smoothly
- It may lead to a reduction in time spent by your professional advisors in working up proposals
- If a proposal is unlikely to be acceptable we can advise you in advance to enable you to suggest amendments or consider alternative proposals

Our charges

All householder enquiries, small scale developments of up to 5 dwellings, general advice on land-use and small commercial developments of up to 500sq metres of commercial space.

We charge £60 per hour with a minimum charge of 1 hour and then at £30 per 30 minutes or part thereof. This includes travel time to site visits if required. The Officer allocated to deal with your pre-application enquiry will be dependant on the nature and scale of the proposals and resources available.

The Planning Officer will advise you at the outset of the estimated cost and will not exceed this without your agreement. Advice will only be provided once the fee, in line with the estimation, has been received.

You can minimise costs by providing as much information about your scheme as possible in advance, but there is no requirement to do this.

Listed Buildings

Proposals which involve Listed Buildings, or affect their setting, will have a minimum charge of £180 to enable specialist advice to be obtained. This charge will be higher if the proposal also requires the involvement of a Planning Officer.

All other applications

Fee

- £500 or 1.5% of the appropriate fee under the Application Fees Regulations, whichever is the greater, for up to an hour long meeting and written response
- If the Planning Officer recommends further time is spent on your proposal we will provide you with an estimate and obtain your agreement.

We also need the following information

- Written details of the address and proposal
- Description of the nature and scale of the development proposed and the uses to which land and buildings are to be put
- Site location plan with the site clearly marked (to a recognised scale, north point etc)
- Sketch drawings providing details of the proposal (to a recognised scale)
- Photographs of the site and surrounding area, with particular regard to any nearby houses or other development which might be affected by your proposal
- Contact details including phone number and email address
- An initial design and access statement
- Access and parking arrangements
- This may also need to be accompanied by ecological, landscape, contamination, flood and transport assessments depending upon the location, nature and complexity of the development.

What the costs cover

These fees cover administration costs and the time spent in research, assessment, a meeting as necessary, and in making a written response.

Subject:	**INFORMATION SECURITY, RISK AND GOVERNANCE FRAMEWORK AND POLICIES**
Meeting and Date:	**Cabinet – 9 January 2017**
Report of:	**David Randall, Director of Governance**
Portfolio Holder:	**Councillor Mike Conolly, Portfolio Holder for Corporate Resources and Performance**
Classification:	**Unrestricted**
Purpose of the report:	This report seeks approval of an Information Security and Governance Framework and an associated suite of Information Governance Policies
Recommendation:	1. The Information Security and Governance Framework and the associated suite of Information Governance Policies at Appendices 3 are approved for implementation retrospectively from 9 January 2017. 2. The Director of Governance is authorised to make any future minor changes or amendments to the Framework and associated policies providing that these changes do not change the substance of any of the policies. 3. That the Director of Governance be appointed as the Senior Information and Risk officer for the Council and be authorised to discharge the functions and responsibilities of that role and that that the Head of Corporate Services be appointed as his deputy.

1. Summary

1.1 In February 2015 the three SIROs (Senior Information Risk Owner) and their deputies of the Councils of Canterbury, Dover and Thanet together with key staff from EKS (ICT), EKHR and EKAP formed the East Kent Corporate Information Governance Group.

1.2 The main objective of the group was to improve the management and security of information held and used by the Councils, provide support to the SIROs and to develop an Information Security and Governance Framework and an associated suite of Information Governance Policies for adoption consistently across the three Councils.

1.3 The overarching framework and associated policies have been subjected to formal consultation with the recognised trade unions through the Collective Bargaining Agreement and in addition there has been consultation directly with all staff.

1.4 Once adopted, alongside the formal launch of the new framework and associated policies, the appropriate training and development will be delivered with the intention of affecting behavioural change.

2. Introduction and Background

2.1 During 2013, the Cabinet Office required each authority to appoint a Senior Information and Risk Owner (SIRO). The role of the SIRO includes:

- Accountability for Information Risk Management, its confidentiality, integrity and availability and to ensure it is being effectively managed and correctly classified
- Leading and encouraging a culture that protects and exploits information within the Council, including agreeing the risk appetite within the Authority
- Responsibility for the corporate information security and information governance policy
- Providing an annual statement of the security of information assets for inclusion in the Annual Governance Assurance Statement

2.2 The Director of Governance has de facto assumed the role of the SIIRO for Dover District Council as the functions of the role closely align with his other responsibilities; he has not however been formally designated or appointed to that role. It is therefore recommended that Cabinet formally appoints the Director of Governance, (incumbent David Randall), to be the SIRO for Dover District Council and authorises him to discharge the functions and responsibilities of the role. It is further recommended that the Head of Corporate Services (incumbent Colin Cook), be appointed as his deputy.

2.3 In February 2015 the three Senior Information Risk Owner and their deputies of the Councils of Canterbury, Dover and Thanet together with key staff from EKS (ICT), EKHR and EKAP formed the East Kent Corporate Information Governance Group.

2.4 The main objective of the group was to improve the management and security of information held and used by the Councils, provide support to the SIROs and to develop an Information Security and Governance Framework and an associated suite of Information Governance Policies for the three Councils.

2.5 Across the three authorities and within EKS (ICT) there were already some information and security policies in place, however many of these were not consistent and/or not up to date, causing some difficulty in their application by the authorities and particularly by EKS (ICT).

2.6 The objectives of the new framework and associated policies are to ensure that each authority is compliant in terms of information governance, has sound policies and manages its information management risks. One of the key risks to all authorities is from an information/data breach resulting in a substantial fine by the Information Commissioner. Forming the Corporate Information Governance Group has utilised the skills and resources within the three authorities; and within EKS (ICT), EKHR and EKAP; and working together the group has developed a suite of consistent policies for each authority and through these we aim to effectively manage our information management and security risks and reduce the risk of a significant information/data breach. The framework and policies all large in volume, have all been written quite concisely, providing increased clarity and understanding for all staff about information management.

2.7 Ultimately, the success of the framework and policies will be measured through a better understanding of the information governance requirements and behavioural change by staff in relation to information management. Appendix 2 provides a short guide to the framework and each of the policies, including an analysis of who and how staff are affected by each policy.

2.8 The Director of Governance and the Head of Corporate Services represented DDC in developing the overarching framework and associated policies, which were consulted on with the recognised trade unions and with staff for 45 days between 13 October 2016 and 27 November 2016. The consultation document was transparent and accessible providing a high level diagrammatic view of the framework and policies, a summary document highlighting the key aspects of each of the policies and also a full set of all of the policies, enabling staff to access at the level that best suited them.

2.9 Feedback and comments from both the Trade Unions and staff were collected via the intranet pages and were considered by the East Kent Corporate Information Governance Group at its meeting on the 2 December 2016. There wasn't a great deal of feedback or comment, but that received has helped inform the final framework and policies at Appendix 3. The End of Consultation document highlighting the changes made following consultation can be found at Appendix 4.

2.10 It is proposed that the framework and policies, are implemented from the date of adoption - 9 January 2017. The framework will be available in digital form on the DDC Intranet, with hyperlinks to all of the associated policies. In addition the Corporate Training Programme will ensure that suitable training is provided to support the introduction of the policies and will then be periodically refreshed.

3. Identification of Options

3.1 The options for Cabinet are:

(a) To approve the Information Security and Governance Framework and the associated suite of Information Governance Policies that have been developed by the East Kent Corporate Information Governance Group and then fully consulted upon with the Recognised Trade Unions. These are being recommended for adoption across the three East Kent councils. This is the preferred option.

(b) Request that the Corporate Information Governance Group develops a different framework and suite of associated policies that still delivers the desired objectives.

(c) Request that this Council develops its own Information Security, Risk and Governance Framework and the associated suite of Information Governance Policies.

4. Evaluation of Options

4.1 The successful development of the framework and these policies for Canterbury City, and Dover and Thanet District Councils; and our East Kent partners at East Kent Services, East Kent HR and East Kent Audit Partnership has demonstrated the value of pooling our skills and resources and working together to develop a common framework and associated policies. It is sensible to develop a consistent approach, especially as the three authorities work in partnership with EKS (ICT), who will be required to apply some of the policies on behalf of each council and will now be able to apply them with consistency.

4.2 East Kent Housing has now joined the Corporate Information Governance Group and will be consulting in early 2017 on this framework and its associated policies, with the intention of adoption. This reinforces the desire to retain a consistent information governance framework and suite of policies for all of East Kent.

4.3 The requested delegation to the Director of Governance to make any future minor changes or amendments to the Framework and associated policies (providing that these changes do not change the substance of any of the policies) will ensure that this Council's framework and policies remain consistent with East Kent partners.

5. Resource Implications

5.1 There are no direct additional resource implications from the proposed framework and associated policies.

6. Corporate Implications

6.1 Comment from the Director of Finance (linked to the MTFP): Finance has been consulted and has no further comment to add (VB).

6.2 Comment from the Solicitor to the Council: The Solicitor to the Council has been consulted in the preparation of this report and has no further comment to make.

6.3 Comment from the Equalities Officer: The report does not specifically highlight any equality implications, however in discharging their responsibilities members are required to comply with the public sector duty as set out in section 149 of the Equality Act 2010 http://www.legislation.gov.uk/ukpga/2010/15

7. Appendices

Appendix 1: A diagrammatical representation of the framework and associated policies.

Appendix 2: A Short Guide to the Information Governance Policies and how they affect them

Appendix 3: The framework and each policy in detail

Appendix 4: End of Consultation Document

Contact Officer: David Randall, Director of Governance

Appendix 1

Diagrammatical Representation of the Framework and Policies

Appendix 2

A Short Guide to Information Governance Policies and How They Affect You

Background

The ever increasing amount of data being generated and stored as part of the way in which we work creates a number of concerns in how we protect this information from unintended or malicious infringements. In order to govern the way in which we operate, a number of new policies have been produced and existing ones updated as new technology is introduced and revised legislation emerges.

In order to keep abreast of the latest developments a Corporate Information Governance Group (CIGG) has been established which is made up of senior staff from each of the three East Kent Councils, East Kent Audit and East Kent ICT to oversee the governance arrangements concerning information security and confidentiality.

Each Council has appointed a Senior Risk Information Office (SIRO) and a deputy SIRO who act as the local CIGG representatives and are charged with the responsibility of ensuring that the information governance arrangements are sound. A major initial task for the CIGG was to review all existing guidance concerning information governance and produce a new suite of policies which are consistent across East Kent. These can be found at Appendix 3.

You are now asked to familiarise yourself with these policies and in order to help you with this there is a summary of each policy and how it affects you below. If you have any questions or concerns please ask the SIRO or Deputy SIRO who for Dover District Council are:

SIRO: David Randall – Director of Governance
Deputy SIRO: Colin Cook – Head of Corporate Services

1. Information Security, Risk and Governance Framework

Summary
This Framework sets out the roles and responsibilities allocated to key staff to protect the Council's information from all threats, whether internal or external, deliberate or accidental, to ensure business continuity and to minimise business damage.

Who is affected?
All staff should be aware of their obligations and the governance structure concerning the security and confidentiality of information.

2. Physical and Environment Security

Summary
This policy concerns the security of access to our buildings and how we protect the information stored in either electronic or paper format. It provides general guidance on how

we can maintain safe and secure buildings through access controls and also reiterates the importance of complying with document retention responsibilities.

Who is affected?
All staff need to know the requirements for everyone to display valid identification when visiting or working at our premises and be aware of the records management principles that apply to the information which they own.

3. Password Policy

Summary
This policy document sets out the minimum standards everyone must adhere to when making decisions about passwords which are a key method in protecting the data for which we are responsible. Good password choices defend the organisation from loss or theft of data and protect you from impersonation and identity theft.

Anyone found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Password testing is performed on a periodic basis; breaches of this policy will be reported as an Information Security Incident.

Who is affected?
All staff need to know the strict access password requirements and the devices and systems to which they apply

4. Internet Use Policy

Summary
This policy outlines your personal responsibilities when using the Council's internet and informs what you must and must not do. All staff must familiarise themselves with the detail, and spirit of this policy before using the internet so that they are aware of the acceptable use of such facilities

Who is affected?
All staff who use the Council's internet.

5. Email Acceptable Use Policy

Summary
This policy provides guidance on the acceptable use of the Council's email system and informs what you must and must not do. Anyone using the Councils email system must familiarise themselves with these details to ensure that they remain within these strict guidelines and the consequences of inappropriate use of the email.

Who is affected?
All users of the Council's email system

6. Wi-Fi Policy

Summary
This policy sets out the standards everyone must adhere to when making decisions about the use of Wi-Fi. Whilst corporate devices such as iPads and smart phones are configured to be secure there is still a user requirement to exercise due care in which Wi-Fi connections should be trusted.

Failure to do so will put you and the organisation at risk from data loss, identity theft and reputational damage. Anyone found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Who is affected?
All staff who use Wi-Fi anywhere to connect any corporate devices.

7. Removable Media and Remote Working Policy

Summary
A removable media device is any device or medium capable of transporting data and includes smartphones, tablets, USB memory sticks, cameras etc. This policy aims to ensure that the use of removable media devices is controlled in order to prevent any unintended or deliberate breach of information security.

Who is affected?
All staff who use a portable device to transport data.

8. Information Management Policy

Summary
The aim of this policy is to establish an effective governance structure to ensure that staff understand their responsibility to handle all data in line with this policy. This is in particular respect to confidentiality, security, integrity and accessibility of information.

Who is affected?
All staff must be aware of this policy and how to protect their data.

9. Incident Management Policy

Summary
This policy will ensure that all incidents that result in the unauthorised disclosure of personal or sensitive data must be reported appropriately to the ICT Helpdesk or the Senior Information Risk Officer.

Who is affected?
All staff must be aware of this policy and how to report an incident.

10. Payment Card Industry Data Security Standards Policy

Summary
The aim of this policy is to ensure all customer payment transactions taken by debit or credit cards are conducted within the strict guidelines set out in the Payment Card Industry Security Standards.

Who is affected?
This requires that all staff involved in administering or managing customer payments familiarise themselves with these guidelines and adhere to them at all times to protect confidential customer account data and the Council's reputation

11. Business Continuity Policy

Summary
The aim of this policy is to ensure that all information held by the Council can be reinstated as soon as possible in the event of a disaster occurring to ensure an unbroken level of

frontline services, whilst full restoration is planned for and implemented. It sets out the responsibilities of designated Information Asset Owners to ensure that specific business continuity plans are in place.

Who is affected?
All staff should be aware of the Council's responsibilities to provide a backup facility in the event of a disaster and the responsibilities of specifically identified officers.

12. Information Risk Management Policy

Summary
The purpose of this policy is to ensure that staff are aware of the types of risks involved in managing information and take the necessary actions to reduce or eliminate them.

Who is affected?
All staff should be vigilant in detecting information risk and familiarise themselves with the risk reporting process.

13. Information Sharing Policy

Summary
Government policy places a strong emphasis on the need to share information across organisational and professional boundaries, in order to ensure effective co-ordination and integration of services. The aim of this policy is to provide a framework to enable the legitimate sharing of data between staff, departments and other agencies and establish a mechanism for this process.

Who is affected?
All staff should be aware of the need to have strict controls over data which is shared with other departments and external agencies.

14. PSN Acceptable Usage Policy and Personal Commitment Statement

Summary
The Public Sector Network (PSN) is a secure private Wide-Area Network (WAN) which enables secure interactions between connected Local Authorities and organisations that sit on the pan-government secure network infrastructure. Some Council staff will be required to have access to the facilities operated on this network in order for them to carry out their business. This may include staff having access to a secure email facility (GCSX email) or the DWP's Customer Information System.

This policy requires staff using the PSN to sign up to the rules relating to secure emails and information usage.

Who is affected?
All staff requiring access to the PSN network in any way will be required to read and understand this Acceptable Usage Policy (AUP) and accept the Personal Commitment Statement.

15. Digital Security Policy – Network Access and Availability

Summary
Protecting the Council's digital information assets is key to delivering the council's digital strategy. A failure of confidentiality, integrity or availability could have a significant effect on

the ability of the council to deliver its services via digital platforms. This policy sets out the minimum requirements for access to the council's digital resources.

Who is affected?
All staff must comply with this policy at all times when accessing the Council systems.

16. Digital Security Policy - Monitoring and Standards

Summary
This policy sets out the standards and requirements that will be adhered to in the operation of the Council's software and infrastructure assets to protect the security of the Council's digital information.

Who is affected?
This policy is particularly relevant for technical IT staff when administering the Council's digital systems.

17. Data Protection Policy

Summary
The aim of this policy is to ensure that understand, and comply with, the eight principles of the Data Protection Act. Everyone has rights with regard to the way in which their personal data is processed. During the course of our activities we collect, store and process personal data about our customers and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation.

Who is affected?
All staff must comply with this policy when processing personal data.

Appendix 3

Information Security, Risk and Governance Framework

- **Introduction**
- **Scope**
- **The Policy**
  - Purpose of the Framework
  - Information/ Information Systems
  - Information Assets
  - Information Risk Management
  - Responsibility for Information Risk Management
  - Roles and Responsibilities

- **Policy Compliance**
  - Document Control

Introduction

This guidance is aimed at those responsible for managing information security, risk and governance within Canterbury, Dover and Thanet councils. It reflects Government guidelines and is consistent with the Cabinet Office report on 'Data Handling Procedures within Government'.

The key requirement is for information security, risk and governance to be managed in a robust way within work areas and not be seen as something that is the sole responsibility of ICT or Information Governance (IG) staff. Assurances need to be provided in a consistent manner. To achieve this, a structured approach is needed. This structured approach relies upon the identification of information assets and assigning 'ownership' of assets to senior accountable staff.

Information is a valuable asset that each council has a duty and responsibility to protect. We acknowledge our responsibility to our community and the expectations placed on each council where information is concerned. The council understands the duty it has under the Data Protection Act 1998 and is monitored and regulated by the Information Commissioner's Office and the Local Government Data Handling Guidelines. As a local authority, each council will comply with the procedures and requirements of the Local Government Data Handling Guidelines.

The Information Commissioner's Office now have powers to enable them to impose monetary penalty notices to organisations for up to £500,000 and £50,000 to individuals for breaches of the Data Protection Act, along with having the authority to carry out assessments of organisations to ensure their processes follow good practice.

To ensure that information assets and information systems are used and managed effectively, efficiently and ethically, the council has produced an Information Security, Risk and Governance Management Framework, to ensure everyone is aware of their obligations.

Scope

The Information Security and Governance Policy and all the supporting documents, apply at each council to all employees, Members of the council, temporary staff, contractual third parties, partners or agents of the council who have access to any information, information systems or information assets for council purposes.

Information Security, Risk and Governance Framework

This Information Security, Risk and Governance Policy is the over-arching document of each council's Information Security, Risk and Governance Management Framework, (see figure 1 below). The framework comprises of the Information Security and Governance Policy and specific supporting procedures, standards and guidelines as follows:

1. Internet Use

2. Information Management

    a. Data Protection

3. Password Policy
4. Physical and Environmental Security
5. Removable Media
6. Information Risk Management
    a. Incident Management.
7. Information Sharing
8. Digital Security
    a. Network Access and Availability
    b. Monitoring Standards
9. Business Continuity
10. Card Payments
11. E-mail, instant messaging and social media
    a. Secure e-mail and Public Services Network (PSN)


Information Security, Risk & Governance
PSN Personal Commitment
Email Use
Internet Use
Information Managment
Data Protection
Physical & Environmental security
Removable Media
Information Risk Managment
Incident Management
Information Sharing
Business Continuity
Password Policy
Network Access/ Availability
Digital Security
Monitoring & Standards
Card Payments

Purpose of the Framework

The purpose and objective of this Information Security, Risk and Governance Framework is to protect the council's information assets from all threats, whether internal or external, deliberate or accidental, to ensure business continuity, minimise business damage and maximise return on investments and business opportunities.

Each council is committed to protecting information through preserving:

Confidentiality

Protecting information from unauthorised access, use and disclosure from unauthorised individuals, entities or processes.

Integrity

Safeguarding the accuracy and completeness of information assets. This may include the ability to prove that an action or event has taken place so that it cannot be repudiated later.

Availability

Being accessible and usable on demand by an authorised individual, entity or process.

Information/ Information Assets

This Information Security and Governance Policy applies to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper
- Information or data stored electronically, including scanned images
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card
- Information stored on portable computing devices including mobile telephones, PDA's and laptops
- Speech, voice recordings and verbal communications, including voicemail
- Published web content, for example intranet and internet
- Cloud and externally hosted data
- Shared data

Information Asset

This Information Security and Governance Policy also applies to information assets, which come in many shapes and forms. Therefore, the following list can only be illustrative. Typical assets include:

Personal Information Content

- Databases and data files.
- Back-up and archive data.

- Audit data.
- Paper records (client case notes and staff records).
- Paper reports.

Software

- Applications and System Software.
- Data encryption utilities.
- Development and Maintenance tools.

Other Information Content

- Databases and data files.
- Back-up and archive data.
- Audit data.
- Paper records and reports.

Hardware

- Computing hardware including PCs, Laptops, PDA, communications devices e.g. I-phones, iPad's and removable media.

System/Process Documentation

- System information and documentation.
- Operations and support procedures.
- Manuals and training materials.
- Contracts and agreements.
- Business continuity plans.

Miscellaneous

- Environmental services e.g. power and air-conditioning.
- People skills and experience.
- Shared service including Networks and Printers.
- Computer rooms and equipment.
- Records libraries.

Information Risk Management

Information security and governance arrangements are the overall process of analysing, evaluating, assessing and mitigating the impact of risks to an organisation's information and information systems. Information risk management includes physical, personnel and information security and is an essential enabler to making councils work efficiently. Information risks must be managed effectively, collectively and proportionately, to achieve a secure and confident working environment.

The council is aware that risks can never be eliminated fully and it has in place a risk strategy that provides a structured, systematic and focused approach to managing risk. However risk management is not about being 'risk averse', it is about being 'risk aware'. Some amount of risk taking is inevitable and necessary if the council is to achieve its objectives.

The council seeks to capitalise on opportunities and to achieve objectives once those decisions are made. By being 'risk aware', the council is in a better position to avoid threats, take advantage of opportunities and ensure its objectives and goals are realised.

Information risk will be managed by assigning roles and responsibilities and co-ordinating the implementation of this policy and all supporting documentation. Together these measures form the Information Risk Management lifecycle and will apply across each council and in their dealings with all partners and third parties.

Responsibility for Information Risk Management

At each council, Senior Management (Directors and Heads of Service) has the responsibility and accountability for managing the risks within their own work areas. Each council will provide guidance and training to its staff to enable them to understand and carry out their responsibilities in respect of security.

Employees have a duty to work safely, avoid unnecessary waste of resources and contribute to risk management initiatives in their own area of activities. The cooperation and commitment of all employees is required to ensure that council information resources are not unlawfully used as a result of uncontrolled risks.

The Local Government Data Handling Guidelines introduce some specific roles in relation to Information Risk Management as follows:

- Accounting Officer.
- Senior Information Risk Owner.
- Information Asset Owners.
- Support Information Asset Owner.
- System Owner.

These specific roles together with the Data Protection Officer and the IT provider will work together with senior management to ensure compliance with best practice as reasonably practicable with the over-riding objective to keep the council's information safe.

Role and Responsibilities

The table below details the roles and responsibilities allocated to key staff:

Accounting Officer	The **Accounting Officer** has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. **(Chief Executive)**
SIRO	The **Senior Information Risk Owner** is familiar with and takes ownership of the organisation's information risk policy and strategy**. (Nominated Director or Head of Service)**

IAO	**Information Asset Owners** are Heads of Service/Managers involved in running the relevant Directorate. Their role is to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of those assets.
SIAO	**Supporting Information Asset Owners** are at Service Unit Level and may have more familiarity with the information assets of that particular area. They are required to feedback to IAO's on what information their service area holds and how it is being managed.
System Owners	**System Owners** are responsible for Information systems. They will ensure system protocols are followed. They have responsibility to recognise actual or potential security incidents, consult their IAO on incident management, and ensure that information systems are accurate and up to date.

The aim is to ensure that the approach to information risk management:

- Takes full advantage of existing authority and responsibility structures where these are fit for this purpose.
- Associates tasks with appropriate management levels.
- Avoids unnecessary impacts on day to day business.
- Ensures that all the necessary activities are discharged in an efficient, effective, accountable and visible manner.

Policy Compliance

If any person or organisation in scope is found to have breached this policy one of the following consequences may be followed;

- Councils' disciplinary procedure.
- Breach of contract.
- Member code of conduct.

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or Senior Information Risk Office.

Document Control		
Title/Version	-	Information Security, Risk and Governance Framework
Owner	-	Corporate Information Governance Group
Date Approved	-	
Review Date	-	
Reviewer	-	

Revision History			
Revision Date	**Reviewer (s)**	**Version**	**Description of Revision**
March 2015	David Randall	1.0	Initial Version
March 2016	Hannah Lynch	1.1	Format Changes
23/09/2016	CIGG	1.2	Final Review

Authority / SIRO	Signature	Date
Canterbury City Council SIRO		
Dover District Council SIRO		
Thanet District Council SIRO		

Physical and Environmental Security Policy

- **Introduction**
- **Scope**
- **The Policy**
  - General Information
  - Out of Hours Access
  - Visitors
  - Contractors
  - Deliveries
  - Emergency Procedures
- **Maintenance of paper Records**
  - Overview
  - Record Retention and Disposal
  - Departmental Responsibilities
- **Policy Compliance**
  - Document Control

Introduction

This policy forms part of the Corporate Information Governance Group policy framework. It supercedes all previous policies on this subject matter.

Scope

This Policy applies to, but is not limited to, all of the councils, Councillors, Employees, Partners, contractual third parties and agents of the councils.

Physical and Environmental Security

General Information

- Always display and present a valid ID card or name badge.
- Challenge anyone who is not wearing a valid ID card or name badge.
- Do not allow anyone into the staff areas who is not displaying a valid ID card.
- Do not allow anyone to use your ID card.
- Never leave personal possessions or sensitive papers unattended. Lock them away or keep them out of sight.
- Do not leave Business Equipment unattended in unsecure locations.
- Close and secure all windows in your immediate work area when you leave the office at night. This is a staff responsibility and must not be left to the cleaners or caretakers.
- Internal staff doors are for staff access only and must be kept closed during public opening hours (8.30am – 5pm)
- External staff entry doors must be kept closed at all times. Do not leave these doors on the catch or prop them open.

Out of hours access

- Please refer to the Out of Hours Access Procedure if you require out of hours access.
- For meetings involving external visitors held outside of public opening hours you will need to make arrangements for your visitors to gain access to the building. It is staff responsibility to ensure visitors are met and escorted to the meeting place and shown out of the building once the meeting has finished.
- Please email prior to the meeting so that arrangements can be made with the on-duty caretaker for locking up the building.

Visitors

- All visitors must be signed in at main reception and issued with a visitor's pass, which they must display.
- When your visitor leaves the building, please ensure they are 'signed out' and their visitor badge is returned.
- If your visitor is here outside of public opening hours (after 5.00pm), you must escort your visitor safely out of the building.
- Remember, you are responsible for your visitors whilst they are in the building. Do not allow your visitor to wander unaccompanied in the staff areas.
- Where enforced, visitors with vehicles will need to display a car park permit from Main Reception if they have been unable to park in the Visitor Space.

Contractors

- All contractors must either display a company ID badge or a temporary contractors ID badge/ card.
- Where enforced, contractors with vehicles will need to obtain a car park permit from main reception, which must be displayed in the vehicle.
- It is also advisable that the company or the individual contractors sign a copy of the confidentiality statement to ensure our information is protected.
- Where provided, contractors must park their vehicles in the designed contractor spaces in the staff car parks.
- If contractors are required to work outside of normal office hours, you must follow the Out of Hours Procedure for contractors.

Deliveries

- Receipt of deliveries and onward movement to other offices are managed through the print and mail room, with the exception of ICT which is delivered directly to ICT.

Emergency procedures

- Each council will have separate policies and procedures for managing an emergency which might impact on the security of council owned buildings and records. Examples include evacuation of the building, dealing with suspicious mail or packages or responding to a bomb threat.

Maintenance of paper records

1. Overview

Each department must manage the council's records to ensure that:

- The council complies with the eight principles of the Data Protection Act 1998;
- Records meet the authority's business needs;
- Records are retained and then destroyed in accordance with departmental retention schedules;
- Records are destroyed using confidential disposal procedures when necessary; and
- The council conforms to any legal and statutory requirements relating to record-keeping.

Each department should have in place a record keeping system (paper or electronic) that documents its functions and provides for quick and easy retrieval of information. It must also take into account the legal and regulatory environment specific to the area of work.

The record keeping system must be maintained so that the records are properly stored and protected, and can easily be located and retrieved. Sensitive information should wherever possible be stored in a lockable cabinet.

2. Record Retention and Disposal

Records should be disposed of in line with the Information management policy. Therefore, departments must have in place clearly defined arrangements for the assessment and selection of records for disposal, and for documenting this work.

The system should ensure that appropriate records are reviewed and disposed of or transferred. Documentation of the disposal/transfer of records must be completed and retained. Records selected for permanent preservation are transferred to the appropriate location within the council's own offices.

3. Departmental responsibilities

1. There should be a clear understanding on the relationship between manual and electronic records. For example the appropriate use of shared folders, personal folders, email folders and paper filing systems. No 'corporate' information should be stored on personal directories or in personal files.

2. All staff should be familiar with the department's records management processes. It is recommended that a named person be responsible for the management of those processes.

3. Each division should have prepared a retention schedule detailing each record series. The retention schedule should state how long the records should be retained in the offices or in the records centre before disposal. It is recommended that records are reviewed against the retention schedule at least once a year.

4. Any sensitive records should be kept in a secure location. Where this is not feasible, staff should be made aware of the sensitivity of the information and be clear who is permitted access.

5. Staff should be made aware of the council's responsibilities under the Access to Information legislation and must comply with the Freedom of Information Act, Environmental Information Regulations and the Data Protection Act. The council is under a duty to respond to requests if the information exists in an accessible format, unless it relates to information which is exempt from disclosure.

Policy Compliance

If any person or organisation in scope is found to have breached this policy one of the following consequences may be followed:-

- Councils' disciplinary procedure.
- Breach of contract.
- Member code of conduct.

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or Senior Information Risk Officer.

Document Control		
Title/Version	-	Physical and Environmental Security
Owner	-	Corporate Information Governance Group
Date Approved	-	
Review Date	-	
Reviewer	-	

Revision History

Revision Date	Reviewer (s)	Version	Description of Revision
	Matthew Archer	1.0	First Draft for Consideration
18/01/2016	Hannah Lynch	1.1	Amended Version
17/03/2016	Dave Randall	1.2	Amended for Final Consideration.
	Hannah Lynch		
23/09/2016	CIGG	1.3	Final Review

Password Policy

- **Introduction**
- **Scope**
- **The Policy**
  - Background
  - Key Messages
  - Responsibilities
  - Policy Detail
  - Password Protection
    1. Mobile Devices
    2. The Main Network Password
    3. Internal Systems
  - Password Standards.
  - Internal only Systems
  - Remote Access
  - Password release policy
  - Supplement for Business Systems
  - Supplement for ICT Systems
  - Application Development Standards

- **Policy Compliance**
  - Document Control

Introduction

This policy forms part of the Corporate Information Governance Group policy framework. It supercedes all previous policy on this subject matter.

Scope

This Policy applies to, but is not limited to, all of the councils, Councillors, Employees, Partners, contractual third parties and agents of the councils.

Password Policy

Background

Passwords are a key method in protecting the data for which we are responsible. Good password choices defend the organisation from loss or theft of data and protect you from impersonation and identity theft. This policy document sets out the minimum standards everyone must adhere to when making decisions about passwords.

Anyone found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Password testing is performed on a periodic basis; breaches of this policy will be reported as an Information Security Incident.

Key Message

Mobile devices, (e.g. phones and tablets) must be protected by a screen lock password. As a minimum, this can be a 4 digit pin or longer if the system supports it. It must be changed every 90 days, or whenever there is a suspicion that the passcode is compromised.

The main network password (also known as the Active Directory Password) must be at least 12 Characters long and contain characters from three of the following four categories:

- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Numbers 0 to 9
- Non-alphabetic characters (for example,!, $, #, %)

The password must be changed at least every 365 days or whenever there is reason to believe the password is compromised. A password generator is available if required which creates passwords that exceed the required standard if you would like some suggestions; this can be found by using the following link Password Generator

Passwords should never be written down or stored on-line without encryption.

Responsibilities

All users will familiarise themselves with this password policy. If you observe a breach of this policy, report it to the ICT Service Desk.

System Administrators will familiarise themselves with the Supplement for Business Systems within this policy.

ICT Staff will familiarise themselves with the Supplement for ICT Systems within this policy.

Policy Detail:

Password Protection Standards:

Always use different passwords from the ones you use in your personal life or for other organisations.

Always use different passwords for the various systems within the organisation.

Do not share your passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential information. (Exceptions to this are during ICT Support sessions, where the password must be changed afterwards)

Passwords should never be written down or stored on-line without encryption.

Do not reveal a password in email, chat, or other electronic communication.

Do not reveal a password on questionnaires or security forms.

If an unauthorised person requests a password, or there are other suspicious circumstances, do not provide the password. Report the request immediately to the ICT Service Desk.

If an account or password compromise is suspected, the password must be changed and the incident reported to the ICT Service Desk promptly.

Password Standards

Mobile Devices

Mobile devices, like iPhones and Tablets must be protected by a screen lock password. As a minimum, this must be a 4 digit pin and require only numbers. Where the Mobile Operating system allows the use of a longer PIN (i.e. 6 Numbers) the longer length must be used. It must be changed every 90 days, or whenever there is a suspicion that it is compromised.

The Main Network Password

Some advice that may help you remember a longer password is that you use three consecutive words with some special characters included; these are very strong and can be easier to remember that a random string of letters and numbers.

For example;

OrangeCatch£Price!

The phrase itself is easier to remember as it is so unusual; it is made a strong password by inclusion of upper and lower case letters with special characters placed between the words.

If you have more than one account, it is permitted to re-use up to two thirds of the password as an “aide memoir” as long as each password is substantially different and changed regularly to extend the above example the following are samples of sufficiently different passwords.

PeachCatch£Price!

AppleCatch£Price!

(NOTE: Do not use any of these examples as passwords!)

Explicit Requirements for the Main Network Password

The password must:

Be at least 12 Characters long and contain characters from three of the following four categories:

- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Numbers 0 to 9
- Non-alphabetic characters (for example,!, $, #, %)

The password must not:

- Be a single word, words or Phrase that are in common usage.
- Contain a sequence of known names i.e. family, pets, friends, co-workers, fantasy characters,
- Computer terms and names, commands, sites, companies, hardware, software,
- Birthdays or other personal information such as addresses and phone numbers.
- Car Registration plates
- Contain any of the above spelled backwards.
- Contain any of the above preceded or followed by a digit (e.g., secret1, 1secret)
- Contain any word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Contain any variation of the word “Password” (e.g. Passw0rd, P455w0rd)

Internal only Systems

For systems which are already protected by the Main Network Password, i.e. they are only available once you have logged on using the Main Network Password, password restrictions can be relaxed and it is not required that this policy is followed. The Business Administrator for that system, in consultation with the Information Asset Owner may choose to allow lower strength passwords more appropriate to the data contained within that system. In many cases, a password will still be required. But it is for the Information Asset Owner to decide and communicate what is appropriate for that system.

Remote Access

Access to the Organisation Networks via remote access (i.e. Citrix) will be controlled using a 2nd factor authentication. (Tokens)

Password Release Policy

Passwords for accounts and systems may only be released or reset once the identity and authority of the requester has been proven. All Users have the authority to request a

password reset for their own account. Line managers can request a password reset for any of their staff that are accountable to them (for when staff are on leave or similar).

All password reset requests must be recorded by ICT. Only one person should know the password beyond what is required to handle a password reset.

Supplement for Business Systems

Within our organisation there are many systems protected by a second password, e.g. Training or Admin Systems. Where these are only available once staff have logged onto the main network using a very strong password, the Information Asset Owner can make a decision to relax the requirements of a strong password if they feel that the information contained within that system does not require that level of protection. In this case, the owner of that Information Asset must communicate their minimum requirements to the users of that service. The IAO should also document the reasons for doing so and conduct regular reviews to establish that it continues to be appropriate.

Supplement for ICT Systems

All system-level passwords with non-expiring passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed at least every 180 days.

Where possible, accounts with non-expiring passwords should not be created, where this is not practical, knowledge of this password must either reside with a single named individual or the password must be created by two members of staff who confidentially create half the password each.

Non expiring passwords (e.g. for Service Accounts) must be a minimum of 21 Characters long. Care should be taken to establish that the service that requires this should be able to survive the password being reset. Additional steps should be taken to limit the activity of the account in question (eg restricting where it can be used). Contact the Network and Security team for advice.

User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.

Where SNMP is configurable, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively.

Default passwords must not be used on any system and must be changed at the earliest possible opportunity.

Where ICT staff have more than one Account for administrative reasons, different passwords must be used on each account.

Occasionally, for troubleshooting purposes an ICT Technician may temporarily change a user’s password to something both the ICT Technician and the user know in order to assist with support or diagnosis as a short term measure. A Service Desk ticket must be raised to

record that this has happened and closed only when the account has had a password set known only to the account holder.

Application Development Standards

Application developers must ensure their programs contain the following security precautions.

Applications:

- Shall support authentication of individual users, not groups.
- Wherever possible, shall not store passwords in clear text or in any easily reversible form shall provide for role management, such that one user can take over the functions of another without having to know the other's password.

Policy Compliance

If any person or organisation in scope is found to have breached this policy one of the following consequences may be followed;

- Councils' disciplinary procedure.
- Breach of contract.
- Member code of conduct.

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or Senior Information Risk Office.

Document Control		
Title/Version	-	CIGG Password Policy 1.0
Owner	-	Corporate Information Governance Group
Date Approved	-	
Review Date	-	
Reviewer	-	

Revision History			
Revision Date	**Reviewer (s)**	**Version**	**Description of Revision**
22/10/2015	Will Causton	1.0	Initial Version
19/01/2016	Hannah Lynch	1.1	Format Changes
23/09/2016	CIGG	1.2	Final Review

Internet Use Policy

- **Introduction**
- **Scope**
- **The Policy**
  - Background
  - Key Messages
  - Risks
  - Policy Details
  - Responsibilities

- **Policy Compliance**
  - Document Control

Introduction

This policy forms part of the Corporate Information Governance Group policy framework. It supercedes all previous policies on this subject matter.

Scope

This Policy applies to, but is not limited to, all of the councils, Councillors, Employees, Partners, contractual third parties and agents of the councils.

Internet Use Policy

Background

Canterbury City Council, Dover District Council, and Thanet District Council (The Councils) provide technology devices, such as PCs, laptops, thin client devices, Blackberrys, iPads, iPhones and other smart devices, together with access to the Internet. This policy will ensure all users of the councils provided internet facilities are aware of the acceptable use of such facilities.

There are a number of legislative requirements that must be adhered to in relation to telephony, IT networks and any specific applications, e-mail and Internet use. The acceptable use policy defines for all users what is acceptable and unacceptable use of council systems and equipment.

This Internet Acceptable Usage Policy should be applied at all times whenever using the councils provided Internet facility. This includes access via any access device including a desktop computer, laptop computer or mobile device. Users are also reminded that comments made on social networking sites, chat rooms etc. are in the public domain and must not bring the councils or their partners into disrepute, or be of a defamatory nature. The councils will not tolerate bullying or harassment of colleagues in any form, this includes via social networking.

This policy outlines your personal responsibilities and informs what you must and must not do.

The Internet facility is made available for the business purposes of the councils. A certain amount of such use must not interfere with is permitted in accordance with the statements contained within this Policy.

Key Messages

- Users must familiarise themselves with the detail, and spirit of this policy before using the Internet.
- Users are responsible for ensuring the security of their account logon-id and password. Individual user log-on id and passwords should only be used by that individual user, and they should be the only person who accesses their Internet account.

- Users must not create, download, upload, display or access knowingly, sites that contain pornography or other material that might be deemed illegal, obscene or offensive.
- Users must assess any risks associated with Internet usage and ensure that the Internet is the most appropriate mechanism for the task.
- At the discretion of your line manager and provided it does not interfere with your work, the councils permit some personal use of the Internet in your own time (for example during your lunch-break).

Risks

The councils recognise that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

- The introduction of viruses and malware on to the councils' ICT network.
- The downloading and/or display of inappropriate or offensive material.
- Information and data security incidents.
- The downloading of unauthorised software.
- Damage to the reputation of The Councils.

Non-compliance with this policy could have a significant effect on the efficient operation of The Councils and may result in financial loss, legal action and/ or an inability to provide necessary services to our customers.

Policy Detail

Remote Use

Users will sometimes need to use council equipment and access the council network when working remotely, whether from their home, offsite or when travelling. Remote users are reminded that this policy applies to them wherever they are using council owned equipment and/or accessing the council network from a non-council device.

Before using or taking council equipment overseas you must seek advice from ICT Services

Personal Use of the Council's Internet Service

At the discretion of your line manager and provided it does not interfere with your work, the councils permit reasonable personal use of the Internet in your own time (for example during your lunch-break or after work) provided this is strictly in accordance with the terms of this policy.

If you are in any doubt about how you may make personal use of the councils' Internet Service you are advised not to do so without first seeking the advice and approval of your line manager.

Such use must not interfere with your council work or the work of the councils. The councils reserve the right to withdraw this privilege if they consider that it is being abused. If excessive personal use is suspected and subsequently proved then managers would be permitted to prevent all personal use and consider disciplinary action.

Personal use of the internet may be withdrawn for operational reasons.

You must be aware that the security systems cannot distinguish between personal and official use of the Internet. Your web access will be subject to the same monitoring processes, and may be revealed to ICT, Audit and your own management or other authorised parties.

You must not use the Internet facilities for any other business or commercial purpose.

Internet Account Management, Security and Monitoring

The councils will provide a secure logon-id and password facility for your network account. EK Services ICT department is responsible for the technical management of this account. You are responsible for the security provided by your account logon-id and password. Only you should know your password and you must be the only person who uses your network account.

The councils have systems in place that can monitor and record all Internet usage. You should be aware that the councils' security systems are capable of recording (for each and every user) each Web site visit, each chat, newsgroup, mailing list or e-mail message and each file transfer into and out of its internal networks. The councils reserve the right to do this at any time. No employee should have any expectation of privacy as to his or her Internet usage. Managers will review Internet activity and analyse usage patterns, and may choose to publicise this data to assure that council Internet resources are devoted to maintaining the highest levels of business use and integrity.

Breach of the regulations referred to in this section may result in disciplinary action being taken against an employee up to and including dismissal. Any action against the employee will follow the councils' disciplinary procedures. Specific analysis of Internet use may be provided in support of any investigation.

A breach of the regulations or this policy may result in legal action being taken against the user.

Things You Must Not Do

Access to the following categories of websites is currently blocked using a URL filtering system:

(This list is not exhaustive and may be amended from time to time.) Some websites may not be automatically blocked by the web filter. Staff should exercise their own discretion and report any misclassifications.

- Dating
- Illegal
- Gambling
- Gaming
- Hate and Discrimination
- Hacking
- Instant Messaging
- Internet Telephony
- Offensive and Tasteless
- Peer-to-Peer Networks (These are generally used to distribute media illegally)
- Pornography and Adult Material
- Proxy Avoidance
- SMS and Mobile Telephony Services

This does not apply to EKServices ICT provided services such as web chat, instant messaging, and internet telephony.

Except where it is strictly and necessarily required for your work, for example ICT audit activity or other investigation, you must not use your Internet account to:

- Create, download, upload, display or access knowingly, sites that contain pornography or other material that might be deemed illegal, obscene or offensive.
- Copy or modify copyright protected material downloaded from the Internet without written authorisation from the copyright holder.
- Subscribe to, enter, or use Peer-to-Peer networks or install software that allows sharing of music, video or image files. If you need further information on Peer-to-Peer networks please contact EKS ICT.
- Subscribe to, enter, or utilise real time chat facilities such as chat rooms, text messenger or pager programs.
- Subscribe to, enter, or use online gaming, or betting sites.
- Subscribe to or enter “money making” sites or enter or use “money making” programs.
- Run a private business.
- Download any software that has not been specifically approved for your use in advance by IT Services.
- Impersonate another person on the internet without his or her express permission.

The above list gives examples of unsuitable usage, but is neither exclusive nor exhaustive. Unsuitable material would include data, images, audio files or video files the transmission of which is illegal under British law, and any other activity that is against the rules, and spirit of this and other council policies.

Responsibilities

It is your responsibility to:

- Familiarise yourself with the detail, essence and spirit of this policy before using the Internet facility provided for your work.
- Assess any risks associated with Internet usage and ensure that the Internet is the most appropriate mechanism to use.
- Know that you may only use the councils' Internet facility within the terms described herein.
- Know that all existing council policies apply to your conduct on the Internet, especially (but not exclusively) those that deal with privacy, misuse of resources, harassment of any kind, information and data security, fraud and the Code of Conduct.
- Remember that comments made on social networking sites, chat rooms etc. are in the public domain and must not bring the councils or their partners into disrepute, or be of a defamatory nature. The councils will not tolerate bullying or harassment of colleagues in any form, this includes via social networking.

It is the responsibility of Line Managers to ensure that the use of the Internet facility:

- Within an employees work time is relevant to and appropriate to The councils' business and within the context of the users responsibilities.
- Within an employee's own time is subject to the rules contained within this document.

Policy Compliance

If any person or organisation in scope is found to have breached this policy one of the following consequences may be followed:-

- Councils' disciplinary procedure.
- Breach of contract.
- Member code of conduct.

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or Senior Information Risk Officer.

Document Control		
Title/Version	-	Internet Use Policy
Owner	-	Corporate Information Governance Group
Date Approved	-	
Review Date	-	
Reviewer	-	CIGG

Revision History			
Revision Date	**Reviewer (s)**	**Version**	**Description of Revision**
25/01/2012	A Waite	1.0	Consolidation of all partners' current policies.
20/02/2012	A Waite	1.1	Inclusion of all comments and changes from the working group.
18/10/2012	Sean Hale	1.2	Document finalised.
09/01/2015	J Brackenborough	1.3	Amendments following review by policy working group.
23/09/2016	CIGG	1.4	Final Review.

Email Acceptable Use Policy

- **Introduction**
- **Scope**
- **The Policy**
  - Background
  - Key Messages
  - Risks
  - Policy Details
  - Responsibilities

- **Policy Compliance**
  - Document Control

Introduction

This policy forms part of the Corporate Information Governance Group policy framework. It supercedes all previous policies on this subject matter.

Scope

This Policy applies to, but is not limited to, all of the councils, Councillors, Employees, Partners, contractual third parties and agents of the councils.

Email Acceptable Use Policy

Background

This policy covers all email systems and facilities that are provided by EK Services for the purpose of conducting and supporting official business activity through the network infrastructure of the organisation and all stand alone and portable computer devices.

This policy is intended for all EK Services partners and includes Councillors, Committees, Departments, Partners, Employees of the council, contractual third parties and agents of the council who have been designated as authorised users of email facilities.

Whilst respecting the privacy of authorised users, each organisation maintains its legal right, in accordance with the Regulation of Investigatory Powers Act 2000, to monitor and audit the use of email by authorised users to ensure adherence to this Policy. Any such interception or monitoring will be carried out in accordance with the provisions of that Act. Users should be aware that deletion of email from individual accounts does not necessarily result in permanent deletion from the ICT systems. It should also be noted that email and attachments may need to be disclosed under the Data Protection Act 1998 or the Freedom of Information Act 2000.

All email prepared and sent from any official business email addresses or mailboxes, and any non- work email sent using EK Services ICT facilities is subject to this policy.

'Organisation' refers to Canterbury City Council, Dover District Council, Thanet District Council, EK Services, and East Kent Housing

Key Messages

The following list is a set of rules about the acceptable use of the organisations email system. Disciplinary action may be taken against individuals who abuse the email facility.

Users must:

- Ensure that all emails that are used to conduct or support official business of the organisation must be sent using an official email account.
- Your email account identifies you as an organisation representative, so you must be aware that the recipients of your messages will assume that you are acting on behalf of your employer.

- Make sure that you do not make any statement or comment which reflects badly on the organisation, or contradicts existing policies.

- Adopt a responsible approach to the content of emails, bearing in mind that emails often need to be as formal as any other form of written correspondence such as a letter.

- Consider whether email is the most appropriate way of communicating the message, particularly when dealing with sensitive matters or where debate is likely.

- Check your incoming email regularly, and ensure that all items that require attention are addressed within the organisations guidelines on service standards.

- Be aware that emails are disclosable in any legal action against the organisation including Freedom of Information or Data Protection requests, and emails, which have been deleted by a user or from the network, may, for a period of time, be recovered.

- Do not enter into a contract via email without following the organisations standard authorisation procedures. A contract entered into via email is likely to be legally binding in the same way as any contract, and users must be careful to avoid using language that might be construed as formally offering or accepting a contractual arrangement unless the correct authorisation procedures have been followed. If in doubt, seek the advice of the internal procurement and/or legal teams first.

- Remember that email correspondence is not private as emails can be easily copied, forwarded or archived without the original sender's knowledge. When drafting any email a user should bear in mind that it may be read by a person other than the designated recipient.

- Remember Email is not a secure medium to send confidential information. The consequences of an email containing sensitive information being sent to an unauthorised person could be a fine from the information commissioner. Other information, if mis-sent, could end up on the front page of a newspaper or be used in legal or other formal proceedings.

- Any emails containing information classified as restricted, protected, confidential or above, or which are to be sent to a GSI recipient must be sent from a GCSx email account.

- If you are away from the office for more than a day, use the system capabilities to inform message senders that you are absent and provide alternative contact points using the ‘out of office’ function, or forward your mail to other officers.

- Avoid the mass distribution/forwarding of messages, which can cause congestion on network systems, and can cause offence to some recipients.

- If you find yourself overwhelmed with unsolicited email (‘spam’), or are unsure about the validity of an email or attachment contact the ICT Service desk – it is possible to

set up controls within the email and network systems to filter out unwanted messages.

- If you need to send an email to a large number of external contacts, or you want to attach a very large document, greater than 50mb, please contact the ICT Service desk to advise them of your proposed action and/ or consider the use of a secure file sharing solution. Please bear in mind that large emails may be blocked by the recipient's email.

- A limited amount of personal use is acceptable, providing it is clear that you are communicating in a private capacity, and that you only use the system outside your working time.

- Note that the volume and content of email messages can be monitored by ICT and Audit. While this is primarily a business tool, the systems cannot distinguish between official and private email traffic, so you must be aware that any personal messages you send or receive may be viewed by other officers.

Risks

The Councils recognise that there are risks associated with users accessing and handling information in order to conduct official council business.

This policy aims to mitigate the following risks:

- The introduction of viruses and malware onto the ICT network
- Damage to the reputation of the organisation
- Users of the system using emails to bully or harass others or for some other improper or discriminatory use
- Information and data security incidents
- The propagation of unwanted Email (spam)

Non-compliance with this policy could have a significant effect on the efficient operation of the councils and may result in financial loss, legal action and/ or an inability to provide necessary services to our customers.

Policy Detail

The objective of this policy is to inform users of the terms under which emails may be used by:

- Providing guidance on expected working practice.
- Highlighting issues affecting the use of email.
- Informing users about the acceptable use of ICT facilities in relation to emails.
- Describing the standards that users must maintain.

- Stating the actions that may be taken to monitor the effectiveness of this policy.
- Warning users about the consequences of inappropriate use of the email service.

This policy covers all email systems and facilities that are provided by EK Services for the purpose of conducting and supporting official business activity through the network infrastructure of the organisation and all stand alone and portable computer devices.

This policy is intended for all EK Services partners and includes Councillors, Committees, Departments, Partners, Employees of the council, contractual third parties and agents of the council who have been designated as authorised users of email facilities.

Whilst respecting the privacy of authorised users, each organisation maintains its legal right, in accordance with the Regulation of Investigatory Powers Act 2000, to monitor and audit the use of email by authorised users to ensure adherence to this Policy. Any such interception or monitoring will be carried out in accordance with the provisions of that Act. Users should be aware that deletion of email from individual accounts does not necessarily result in permanent deletion from the ICT systems. It should also be noted that email and attachments may need to be disclosed under the Data Protection Act 1998 or the Freedom of Information Act 2000.

Responsibilities

It is your responsibility to:

- Familiarise yourself with the detail, essence and spirit of this policy before using the email facility provided for your work.
- Assess any risks associated with email usage and ensure that the email is the most appropriate mechanism to use.
- Know that you may only use the councils' email facility within the terms described herein.
- Know that all existing council policies apply to your conduct when using email , especially (but not exclusively) those that deal with privacy, misuse of resources, harassment of any kind, information and data security, fraud and the Code of Conduct.
- The councils will not tolerate bullying or harassment of colleagues in any form, this includes via social networking.

It is the responsibility of Line Managers to ensure that the use of the email facility:

- Within an employees work time is relevant to and appropriate to the councils' business and within the context of the users responsibilities.
- Within an employee's own time is subject to the rules contained within this document.

Policy Compliance

If any person or organisation in scope is found to have breached this policy one of the following consequences may be followed:-

- Councils' disciplinary procedure.
- Breach of contract.
- Member code of conduct.

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or Senior Information Risk Officer.

Document Control		
Title/Version	-	Internet Use Policy
Owner	-	Corporate Information Governance Group
Date Approved	-	
Review Date	-	
Reviewer	-	CIGG

Revision History			
Revision Date	**Reviewer (s)**	**Version**	**Description of Revision**
April 2011	A Waite	1.0	First Draft of combined policies developed by EK services working group.
03/05/2011	A Waite	1.1	Amendments following client group review.
31/07/2012	A Waite	1.2	Amendments following review by policy working group
09/01/2015	J Brackenborough	1.3	Amendments following review by policy working group.
23/09/2016	CIGG	1.4	Final Review.

Wi-Fi Policy

- **Introduction**
- **Scope**
- **The Policy**
  - Background
  - Key Messages
  - Policy Details
  - Responsibilities

- **Policy Compliance**
  - Document Control

Introduction

This policy forms part of the Corporate Information Governance Group policy framework. It supercedes all previous policies on this subject matter.

Scope

This Policy applies to, but is not limited to, all of the councils, Councillors, Employees, Partners, contractual third parties and agents of the councils.

Wi-Fi Policy

Background

The use of Wi-Fi to connect to the Internet has become an essential business enabler. For some devices, it is the only way they can gain onward access to corporate data and resources.

Whilst corporate devices [iPads, etc.] and services [e.g. Email] are configured to be secure [Passwords, encryption, secure connections], there is still a user requirement to exercise due care in which Wi-Fi connections should be trusted.

Failure to do so will put you and the organisation at risk from data loss, identity theft and reputational damage. This policy document sets out the standards everyone must adhere to when making decisions about the use of Wi-Fi.

Anyone found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Key Message

Wi-Fi connections can be classified as one of two types: Direct Connections and Captive Portals.

Direct Connections

The best example of this would be like a home Wi-Fi network provided by your broadband connection. You select the Wi-Fi network, enter any password and connect straight to the Internet.

Captive Portals

These connections take you to a ‘landing page’ [like a registration page] and broker your connection to the Internet.

Whilst the majority of Wi-Fi networks are safe to use, Malicious Actors can and do set up Wi-Fi networks of either type that can try to read your data, exposing you to the risks above. This happens in the UK and abroad; in some foreign countries the deliberate interception of data is a state-sponsored activity.

You must satisfy yourself that the connection is trustworthy, before you connect to it.

Policy Detail

Passwords

Most, but not all, Wi-Fi networks are password protected - this should be considered as a 'network privacy' control and not any guarantee of data security.

Examples of trustworthy Wi-Fi networks

EKS Unify - our 'corporate' Wi-Fi network.

Home Broadband Wi-Fi___33 connections provided by telecoms companies e.g. BT, Virgin, and Sky - reputable companies.

Public Wi-Fi services provided by telecoms companies e.g. VFast, BTOpenzone, O2, and The Cloud. These are good examples of Captive Portal services - where you have to be a member, or take up a subscription.

Other Kent authorities also operate Wi-Fi networks, such as Oakwood House [Speedway] and these are trustworthy.

Examples of non-trustworthy Wi-Fi networks

Web Cafes are non-trustworthy. Whilst this is a broad-brush statement, it represents a reasonable position for data protection needs.

Non-EU countries warrant varying levels of trust, between limited trust [access only non-sensitive data] to no trust [expect all data to be read/stolen].

The same considerations can be extended to wired connections in those circumstances.

Before travelling abroad you should also check your council's policies as regards taking equipment overseas, insurance and accessing data outside of the UK. Consult your line manager for additional guidance.

Responsibilities

You must consider the sensitivity, size and nature of the information being sent or received in determining whether the connection is appropriate before you connect to any Wi-Fi network.

Policy Compliance

If any person or organisation in scope is found to have breached this policy one of the following consequences may be followed;

- Councils' disciplinary procedure.
- Breach of contract
- Member code of conduct

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or Senior Information Risk Owner

Document Control		
Title/Version	-	Wi-Fi Policy
Owner	-	Corporate Information Governance Group
Date Approved	-	
Review Date	-	
Reviewer	-	CIGG

Revision History			
Revision Date	**Reviewer (s)**	**Version**	**Description of Revision**
17/03/2016	Timo Bayford	1.0	Initial Draft for Consideration
24/03//2016	Hannah Lynch	1.1	Amended Version
23/09/2016	CIGG	1.2	Final Review

Removable Media Policy

Contents:

- **Introduction**
- **Scope**
- **The Policy**
  - Background
  - Key Messages
  - Policy Detail
  - Responsibilities
- **Policy Compliance**
  - Document Control

Corporate Information Governance Group.
Removable Media Policy

Introduction

This policy forms part of the Corporate Information Governance Group policy framework. It supercedes all previous policies on this subject matter.

Scope

This Policy applies to, but is not limited to, all of the Councils, Councillors, Employees, Partners, contractual third parties and agents of the Councils.

Removable Media

Background

The Councils' recognise that there are genuine and potentially significant risks associated with the use of Removable Media.

This policy aims to ensure that the use of removable media devices is duly considered, controlled and authorised.

This policy aims to mitigate the following risks:

- The loss of information, regardless of cause; i.e. through theft, loss or negligent use of removable media devices.
- Infection of Council networks or equipment through the introduction of viruses through the transfer of data from one form of IT equipment to another.
- Potential sanctions against the Council or individuals imposed by the Information Commissioner's Office as a result of information loss or misuse.
- Potential legal action against the Council or individuals as a result of information loss or misuse.
- Council reputational damage as a result of information loss or misuse.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

A removable media device is any device or medium capable of transporting data, so includes, but is not restricted to the following:

- iPhones/smart phones
- iPads/tablets
- CDs/DVDs
- Optical Disks
- External Hard Drives
- USB Memory Sticks (also known as pen drives or flash drives)
- Media Card Readers
- Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards)

- MP3 Players
- Digital Cameras
- Backup Cassettes
- Audio Tapes (including Dictaphones and Answering Machines)

Key Messages

- Avoid the use of removable media wherever possible.
- Data stored on removable media devices must be encrypted.
- Data may only be temporarily stored on removable media; it must not be the only copy.
- Removable media devices that are no longer required, or have become damaged, must be handed to ICT.
- Returning or Visiting removable media must be scanned by ICT before being connected to council equipment.
- USB Storage (pen or disk drives etc.) must be procured via ICT.
- If in doubt, seek advice.

Policy Detail

Use of Removable Media presents some significant challenges to the Confidentiality, Integrity and Availability of the council's digital assets. This policy sets out guidance so that when removable media must be used, it is used safely and in compliance with the law.

The recommendation is that removable media is not used and that alternatives should be favoured whenever possible. However, the councils recognise that there are times where its use is the only practical solution. This policy sets out what measures must be taken to protect the council's digital assets where the use of removable media cannot be avoided.

Removable media is a catch all term for a range of devices and technologies. Some protection measures outlined in this policy may not apply to all devices. You should exercise your common sense in the use of removable media, if you are unclear at any point, seek advice from ICT.

Use of removable media is monitored.

Avoid the use of removable media wherever possible.

There are many ways to transfer data without using removable media; Email is the most common and recommended method, especially for smaller data sets. For larger data sets, shared regularly, there are varying options across the councils such as Citrix Sharefile and Corporate Google storage. If you are unsure what options are available to you, please contact the ICT Service Desk for details.

For sharing and collaboration within the organisations, a folder on the shared network is appropriate. Contact the ICT service desk about establishing a safe shared location on the "R" Drive as this storage location is available across the partnership. Do not attempt to create you own R Drive folder, as this would be open to everyone to access.

If you need to work on a document at home, use your work laptop and Citrix. Remember you are not allowed to connect your own personal removable media device to council equipment, and you should not be accessing council systems from a personal device.

There may be genuine operational reasons to store personal or sensitive information on your laptop hard drive i.e. for Business Continuity; this must always be maintained at the current version. If the information can reasonably be accessed via normal remote working tools, then this should be the default method.

Taking documents home on a USB Stick to work on, on your home computer is expressly prohibited. Similarly, you must not email documents to a personal email address or use personal Cloud storage solutions e.g. OneDrive or Google Drive.

You are strongly advised never to save files containing personal or sensitive data to removable media, where this is unavoidable you should contact the ICT Service Desk for advice.

Council data must remain on and only be accessed by council approved equipment.

You are encouraged to seek advice from the ICT Service Desk about alternative solutions.

Data stored on removable media devices must be encrypted.

Removable media can be lost or stolen; if that happens the data on it is at risk. The Data Protection Act requires that you take reasonable steps to protect personal and sensitive data.

This is where the requirement for data encryption arises. This way, if the device is lost, the only loss is the physical device - the data is not considered as having been compromised.

Losing data could result in a fine of up to £500,000, damage to the council's reputation and be damaging for any individuals affected by the loss. By encrypting that data we are removing that risk.

A printed document is media that is removable but encrypting a piece of paper would obviously not be practical. An appropriate measure could be to place it in a sealed envelope and sent by a "signed for" service.

Digital media must always be encrypted. If you need advice about this, contact the ICT service desk.

Data may only be temporarily stored on removable media; it must not be the only copy.

If there is only one copy of the data and it's stored on removable media, there is a risk that data will be permanently lost if that media breaks. All council data should be stored on the network and copies transferred to the removable media.

Much of the council's data is subject to the Freedom of Information Act. If we hold the information, we are obliged to produce it if requested. Similarly, a citizen may make a Subject Access Request [part of the DPA]. If that data is not stored on the network, it cannot be found by a search and we would be in breach of these legal obligations.

Returning or Visiting removable media must be scanned by ICT before being connected to council equipment.

Sometimes, removable media from outside our organisation is brought in and needs to be used. Perhaps a contractor has some data on a CD, or a visitor has brought in a presentation on a USB stick. In this case, it's important to have that scanned by ICT before it's connected.

All digital removable media has the ability transfer computer viruses between the devices they visit [are connected to]. It's possible that even your council approved USB stick could become infected, if it has visited something that's infected. Perhaps you took a presentation to another organisation and it was plugged into the laptop that drives the projector. For this reason any "returning" removable media also needs to be scanned.

Other UK local authorities have suffered £500,000 losses and had to shut down their networks for weeks to resolve virus infections, please take the time to contact the ICT Service Desk.

Responsibilities

All staff are responsible for:

- Only using devices supplied/approved by ICT.
- Securely handling and storing removable media devices.
- Ensuring that all data stored on removable media devices is encrypted.
- Contacting ICT if a removable media device is damaged or faulty.
- Removing all data from the device as soon as practical and prior to disposal.
- Returning devices to ICT when they are no longer needed.
- Reporting any actual or suspected breaches via the Incident Management Process promptly after they are noticed.

Policy Compliance

If any person or organisation in scope is found to have breached this policy one of the following consequences may be followed:-

- Council's disciplinary procedure.
- Breach of contract.
- Member code of conduct.

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or Senior Information Risk Officer.

Document Control		
Title/Version	-	Removable Media
Owner	-	Corporate Information Governance Group
Date Approved	-	
Review Date	-	
Reviewer	-	CIGG

Revision History			
Revision Date	**Reviewer (s)**	**Version**	**Description of Revision**
21/03/2016	Sophie Chadwick Tim Howes	1.0	First Draft for Consideration
23/09/2016	CIGG	1.1	Final Review
28/9/2016	Will Causton	1.2	Redrafting following review

Information Management

- **Introduction**
- **Scope**
- **The Policy**
  - Key Messages
  - Risks
  - Policy Detail
  - Responsibilities

- **Policy Compliance**
  - Document Control

Appendix1 – Information Asset Owners for the Council

Introduction

This policy forms part of the Corporate Information Governance Group policy framework. It supercedes all previous policies on this subject matter.

Scope

This Policy applies to, but is not limited to, all of the councils, Councillors, Employees, Partners, contractual third parties and agents of the councils.

Information Management

Key Messages

The aim of this policy is to establish an effective governance structure to ensure that the council takes information management seriously and all staff understand their responsibility to handle all data in line with this policy.

The councils have a duty of care for the information they process. There are legal responsibilities under the 1998 Data Protection Act as set out in the eight Data Protection Principles. In particular, the seventh principle refers to the council's responsibility in protecting personal data as follows:

'Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data'

Risks

Consequences of poor information management or noncompliance with legislation may result in;

- Loss of Business and Efficiency.
- Reputational Damage.
- Financial Penalties.
- Damage to Integrity of information.

Policy Detail

This policy is intended to ensure:-

- Confidentiality is maintained and information is kept safe and secure
- Integrity is maintained and information remains accurate and unaltered
- Availability is maintained and information is available to be accessed by authorised users.

Responsibilities

- **Corporate Information Governance Group**

To advise each authority's SIRO, to review and update the information and security policies for the three authorities, to effectively manage information and security risks and to monitor and report via the SIROs any security breaches.

- **Senior Information Risk Owner**

The SIRO implements and leads the Information Governance (IG) risk assessment and management processes within the organisation and advises on the effectiveness of information risk management across the organisation.

- **Information Asset Owners**

The Information Asset Owner, who should be a system user of appropriate seniority, must ensure that:-

1. Information is being lawfully processed.
2. Access controls are in place, which are appropriate to the sensitivity of the information used by the system.
3. The major risks which may threaten the Confidentiality, Integrity and Availability of the information are identified and, where possible, mitigated;
4. Instances of misuse or abuse of the system are reported as per the Information Incident Reporting Policy.
5. The integrity of information is verified.

- **Staff**

All staff are personally responsible for securely handling any information that is entrusted to them in line with legislative and business requirements.

All staff should undertake data protection training to understand their responsibilities.

All staff will be an information asset owner for anything held on their individual electronic files in their personal area on the system (i.e. 'g' drive).

Information Asset Register

An information asset is any data that is organised and managed as a single entity.

This could be held on paper or in a computerised system.

- Each organisation will establish a register of all their information assets.
- The SIRO will ensure the information asset register is reviewed annually.

Protective Marking and Classification

The information that is created or processed by the councils is classed as OFFICIAL under the Government Security Classifications Policy. Therefore there is no requirement to protectively mark anything as OFFICIAL information.

There will be examples of information which is not disclosable for legislative reasons e.g. Local Government Act, Data Protection Act, and The Freedom of Information Act and some sensitive personal financial information.

You can, when sharing information, include a handling requirement such as “Do not distribute” or “Commercially Sensitive”.

Policy Compliance

If any person or organisation in scope is found to have breached this policy one of the following consequences may be followed:-

- Councils' disciplinary procedure.
- Breach of contract.
- Member code of conduct.

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or Senior Information Risk Officer.

Document Control		
Title/Version	-	Information Management Policy
Owner	-	Corporate Information Governance Group
Date Approved	-	
Review Date	-	
Reviewer	-	CIGG

Revision History			
Revision Date	**Reviewer (s)**	**Version**	**Description of Revision**
15/10/2015	Dave Randall Sophie Chadwick Will Causton Matthew Archer Hannah Lynch Clare Grant	1.0	First Draft for Consideration
23/09/2016	CIGG	1.1	Final Review

Appendix One

Information Asset Owners for the Council

Incident Management Policy

- **Introduction**
- **Scope**
- **The Policy**
  - Background
  - Key Messages
  - Risks
  - Policy Detail
  - Responsibilities

- **Policy Compliance**
  - Document Control

Introduction

This policy forms part of the Corporate Information Governance Group policy framework. It supercedes all previous policies on this subject matter.

Scope

This Policy applies to, but is not limited to, all of the councils, Councillors, Employees, Partners, contractual third parties and agents of the councils.

Incident Management Policy

Background

Legislation and Compliance obligations require a robust and documented methodology to deal with Information Incident Management. This policy will ensure the council's react appropriately to any actual or suspected incidents relating to information systems and information within the custody of the councils. All staff must be aware of this policy and how to report an incident.

The CIGG will review incident reports and take appropriate action to prevent similar incidents occurring and/or improve systems for the protection of data.

Key Messages

All staff should report any incidents or suspected incidents immediately by informing the ICT Helpdesk via 01227 862043 or by emailing ictservicedesk@ekservices.org

See Appendix 1 for the Incident Management Process flow chart

All incidents that result in the unauthorised disclosure of personal or sensitive data must be reported to the CIGG. The responsible Senior Information Risk Officer, may inform the Information Commissioner's Office.

Incidents that result in a breach to the network may be reported by the EK Services Network and Security Manager to appropriate bodies.

Risks

The CIGG recognises that there are risks associated with users accessing and handling information in order to conduct official council business.

This policy aims to mitigate these risks:

- To reduce the impact of information security breaches by ensuring incidents are followed up correctly.
- To help identify areas for improvement to decrease the risk and impact of future incidents.

Non-compliance with this policy could have a significant effect on the efficient operation of the council and may result in financial loss and an inability to provide necessary services to our customers.

Policy Detail

This policy needs to be applied as soon as information systems or data are suspected to be, or are actually affected by an adverse event which is likely to lead to a security incident.

An “information management security incident” is an adverse event that has caused or has the potential to cause damage to the organisation’s assets, reputation and / or personnel. Incident management is concerned with intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems and processes. It may include ICT equipment but also applies to paper records, letters and any other way data is stored or processed.

An Information Security Incident includes, but is not restricted to, the following:

- The loss or theft of data or information.
- The transfer of data or information to those who are not entitled to receive that information.
- Attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system.
- Changes to information or data or system hardware, firmware, or software characteristics without the Council's knowledge, instruction, or consent.
- Unwanted disruption or denial of service to a system.
- The unauthorised use of a system for the processing or storage of data by any person.

Examples of some of the more common forms of Information Security Incidents have been provided in Appendix 2.

The record of all incidents will be managed by EK Services ICT. Anyone involved in an incident are required to work with ICT to produce that record so that it may be reported to the CIGG.

Resolution of Incidents that do not involve ICT will be managed by the organisations Senior Information Risk Officer.

Resolution of Incidents involving ICT will be managed EK Services ICT.

For full details of the procedure for incident handling please refer to Appendix 3.

Incidents need to be reported at the earliest possible stage as they need to be assessed by a member of the IT Services team.

Responsibilities

All staff should report any incidents or suspected incidents immediately by informing the ICT Service Desk via 01227 862043 or by emailing ictservicedesk@ekservices.org.

EK Services ICT will manage the incident reporting mechanism, where an incident involves ICT equipment; ICT will manage the incident to its operational conclusion.

All incidents that result in the unauthorised disclosure of personal or sensitive data must be reported to the CIGG. The responsible Senior Information Risk Officer, may inform the Information Commissioners Office.

Incidents that result in a breach to the network may be reported by the EK Services Network and Security Manager to Gov-Cert UK, Kent Warp or PSN SIRO.

Policy Compliance

If any person or organisation in scope is found to have breached this policy one of the following consequences may be followed;

- Councils' disciplinary procedure.
- Breach of contract.
- Member code of conduct.

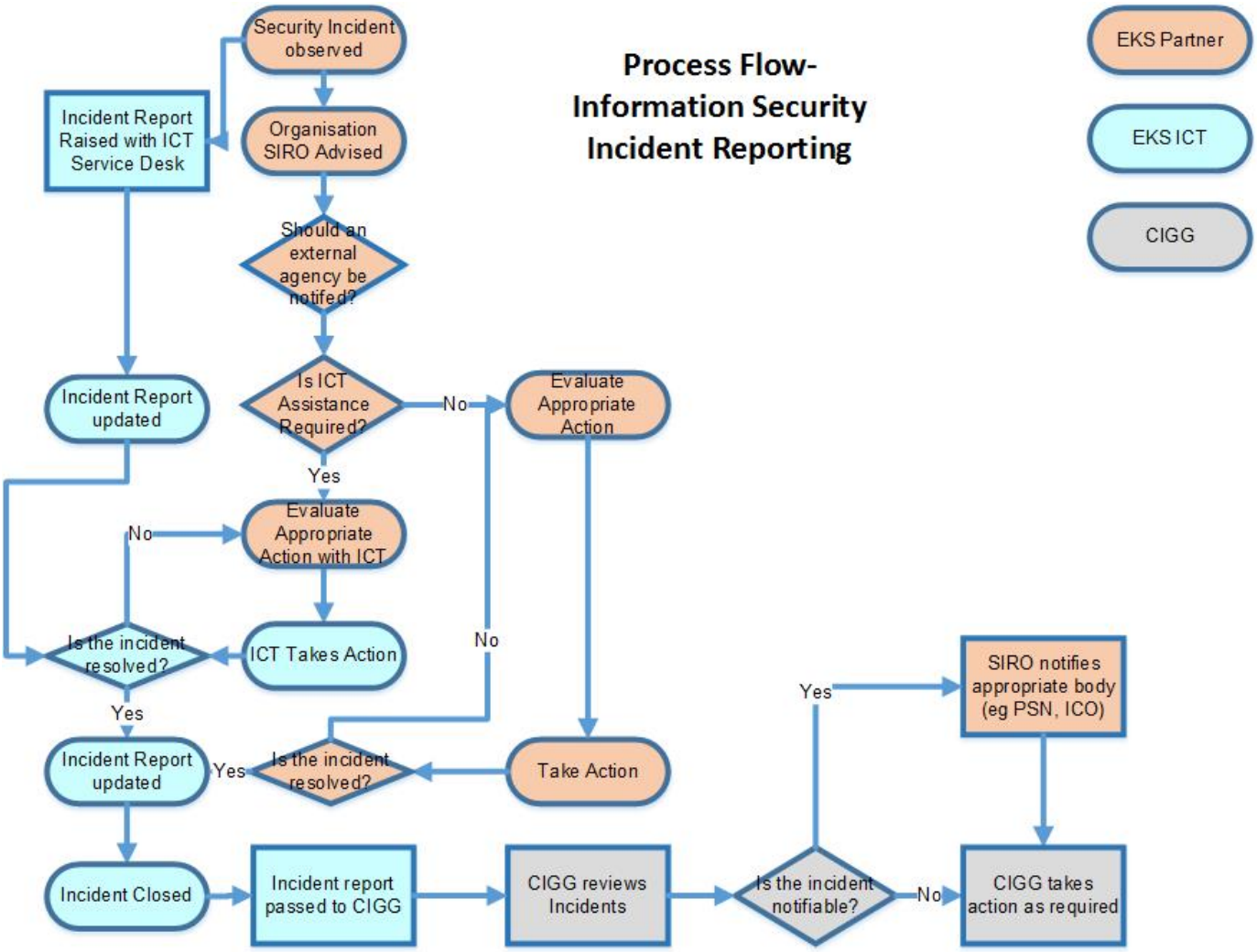
If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or Senior Information Risk Officer.

Document Control		
Title/Version	-	Incident Management Policy
Owner	-	Corporate Information Governance Group
Date Approved	-	
Review Date	-	
Reviewer	-	CIGG

Revision History

Revision Date	Reviewer (s)	Version	Description of Revision
12/12/2015	Will Causton	1.0	Initial Version
15/03/2016	Will Causton	1.1	Draft following CIGG Consultation
23/09/2016	CIGG	1.2	Final Review

Appendix 1


Process Flow-
Information Security
Incident Reporting
EKS Partner
EKS ICT
CIGG
Security Incident observed
Incident Report Raised with ICT Service Desk
Organisation SIRO Advised
Should an external agency be notifed?
Incident Report updated
Is ICT Assistance Required?
No
Evaluate Appropriate Action
Yes
No
Evaluate Appropriate Action with ICT
Is the incident resolved?
ICT Takes Action
No
Yes
Incident Report updated
Yes
Is the incident resolved?
Take Action
Yes
SIRO notifies appropriate body (eg PSN, ICO)
Incident Closed
Incident report passed to CIGG
CIGG reviews Incidents
Is the incident notifiable?
No
CIGG takes action as required

Appendix 2

Examples of Information Security Incidents

Examples of the most common Information Security Incidents are listed below. It should be noted that this list is not exhaustive.

Malicious

- Giving information to someone who should not have access to it - verbally, in writing or electronically.
- Computer infected by a Virus or other malware.
- Sending a sensitive email or letter to the wrong person.
- Receiving unsolicited mail of an offensive nature.
- Receiving unsolicited mail which requires you to enter personal data.
- Finding data that has been changed by an unauthorised person.
- Receiving and forwarding chain letters – including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others.
- Unknown people asking for information which could gain them access to council data (e.g. a password or details of a third party).

Misuse

- Use of unapproved or unlicensed software on council equipment.
- Accessing a computer using someone else's authorisation (e.g. someone else's user id and password).
- Writing down your password and leaving it on display / somewhere easy to find.
- Printing or copying confidential information and not storing it correctly or confidentially.

Theft / Loss

- Theft / loss of a hard copy file.
- Theft / loss of any council computer equipment.

Appendix 3

Procedure for Incident Handling

Reporting Information Security Events or Weaknesses

The following sections detail how users and IT Support Staff must report information security events or weaknesses. Appendix 1 provides a process flow diagram illustrating the process to be followed when reporting information security events or weaknesses.

Reporting Information Security Events for all Employees

Security events, for example a virus infection, could quickly spread and cause data loss across the organisation. All users must understand, and be able to identify that any unexpected or unusual behaviour on the workstation could potentially be a software malfunction. If an event is detected users must:

- Note the symptoms and any error messages on screen.
- If a computer virus infection is suspected, the computer must be immediately powered down or disconnected from the network.
- Not use any removable media (for example USB memory sticks) that may also have been infected.

All suspected security events should be reported immediately to the ICT Service Desk via 01227 862043 or by emailing ictservicedesk@ekservices.org.

If the Information Security event does not involve ICT equipment, or example personal information files that may have been stolen from a filing cabinet, this must be reported to the organisations Senior Information Risk Officer as well as the ICT Service Desk.

The ICT Service Desk will require you to supply further information, the nature of which will depend upon the nature of the incident. However, the following information must be supplied.

- Contact name and number of person reporting the incident.
- The type of data, information or equipment involved.
- Whether the loss of the data puts any person or other data at risk.
- Location of the incident.
- Inventory numbers of any equipment affected.
- Date and time the security incident occurred.
- Location of data or equipment affected.

- Type and circumstances of the incident.

Reporting Information Security Weaknesses for all Employees

Security weaknesses, for example a software malfunction, must be reported through the same process as security events. Users must not attempt to prove a security weakness as such an action may be considered to be misuse.

Weaknesses reported to application and service providers by employees must also be reported internally to the ICT Service Desk. The service provider's response must be monitored and the effectiveness of its action to repair the weakness must be recorded by EK Services ICT reporting outcomes to the CIGG.

Reporting Information Security Events for ICT Staff

Information security events and weaknesses must be reported to the Technical Systems Manager and/or the Network and Security Manager as quickly as possible. A work order must be opened immediately in the ITSM system and the affected organisations SIRO notified, (see Appendix 4).

Security events can include:

- Uncontrolled system changes.
- Access violations – e.g. password sharing.
- Breaches of physical security.
- Non-compliance with policies.
- Systems being hacked or manipulated.

Security weaknesses can include:

- Inadequate firewall or antivirus protection.
- System malfunctions or overloads.
- Malfunctions of software applications.
- Human errors.

Responsibilities and Procedures

Management responsibilities and appropriate procedures must be established to ensure an effective response against security events.

For incidents that do not involve ICT, The Senior Information Risk Officer must decide when events are classified as an incident and determine the most appropriate response. EK Services will record and report the Incident to the CIGG on behalf of the SIRO.

For incidents that involve ICT, EK Services ICT Management will decide when events are classified as an incident and determine the most appropriate response. EK Services will record and report the Incident to the CIGG on behalf of the SIRO.

The incident management process must include details of:

- Identification of the incident, analysis to ascertain its cause and vulnerabilities it exploited.
- Limiting or restricting further impact of the incident.
- Tactics for containing the incident.
- Corrective action to repair and prevent reoccurrence.
- Communication across the council to those affected.

The officer responsible for an incident should risk assess the incident based on the Risk Impact Matrix (please refer to Appendix 4). If the impact is deemed to be high or medium this should be reported immediately to organisation SIRO.

Learning from Information Security Incidents

To learn from incidents and improve the response process incidents must be recorded and a Post Incident Review conducted. The following details must be retained:

- Types of incidents.
- Volumes of incidents and malfunctions.
- Costs incurred during the incidents.

The information must be collated and reviewed on a regular basis by the CIGG and any patterns or trends identified. Any changes to the process made as a result of the Post Incident Review must be formally noted in the minutes of the CIGG

Appendix 4

Senior Information Risk Officers by Organisation.

Thanet District Council, EK Services:
Tim Howes Director of Corporate Governance & Monitoring Officer
tim.howes@thanet.gov.uk
Deputy Siro

Canterbury City Council:
Velia Coffey, Deputy Chief Executive
Velia.Coffey@canterbury.gov.uk
Deputy Siro
Matthew Archer: matthew.archer@canterbury.gov.uk

Dover District Council, EK Human Resources
David Randall, Director of Governance
David.Randall@dover.gov.uk
Deputy Siro
Colin Cook: Colin.Cook@dover.gov.uk

Appendix 5 Impact Matrix: To decide on the potential or actual impact of an information security incident, the impact matrix below should be used

Type of Impact	Reputational Media and Member Damages	Reputational Loss within Government and / or Failure to Meet Statutory / Regulatory Obligations	Contractual Loss	Failure to meet Legal Obligations	Financial Loss / Commercial Confidentiality Loss	Disruption to Activities	Personal Privacy Infringement
Low	None	None	None	None	None	None	None
	Contained internally within the council Unfavorable council member response	Internal investigation or disciplinary involving one individual	Minor contractual problems / minimal SLA failures/	Civil lawsuit / small fine - less than £10K	Less than £100,000	Minor disruption to service activities that can be recovered	Personal details revealed or compromised within department
Medium	Unfavorable local media interest Unfavorable council member response	Government authorised investigation by nationally recognised body or disciplinary involving 2 to 9 people	Significant client dissatisfaction. Major SLA failures. Failure to attract new business	Less than £100K Damages and fine	£100,000 - £500,000	Disruption to service that can be recovered with an intermediate level of difficulty. One back up not backing up for 2 or more days	Personal details revealed or compromised internally within authority. Harm mental or physical to one members of staff or public
High	Sustained local media coverage, extending to national media coverage in the short term	Government intervention leading to significant business change. Internal disciplinary involving 10 or more people	Failure to retain contract(s) at the point of renewal	Greater than £100K damages and fine	£500,000 - £1,000,000	Major disruption to service which is very difficult to recover from. Two or more systems not being backed up for two or more days	Severe embarrassment to individual(s)
	Sustained unfavorable national media coverage	Service or product outsourced through Government intervention	Client contract(s) cancelled	Over £1M damages and / or fine Custodial sentence(s) imposed	More than £1,000,000	Catastrophic disruption - service activities can no longer be continued	Detrimental effect on personal & professional life OR large scale compromise affecting many people. Harm mental or physical to two or more members of staff or public

Payment Card Industry Data Security Standards Policy

- **Introduction**
- **Statement of Applicability**
- **Definitions**
  - What is Cardholder Data?
  - What is Sensitive Information?
- **Approach to PCI DSS Compliance**
- **Requirements**
  - Firewall configuration
  - System Passwords and Security Parameters
  - Protect Stored Cardholder Data
  - Transmission of Cardholder Data
  - Protection of Systems
  - Secure Systems and Applications
  - Access to Cardholder Data
  - Access to Systems
  - Physical Access to Cardholder Data
  - Monitoring and Testing Network Access
  - Testing Security Systems
  - Information Security Policy Maintenance
- **Policy Compliance**
  - Document Control
- **Appendix A**

1. Introduction

As an organisation that takes payments by debit and credit cards, we must comply with a set of standards to ensure the security of the card information. The standards are known as the Payment Card Industry Data Security Standards (PCI DSS), and they apply to organisations around the world. They are set out by the Payment Card Industry Security Standards Council (PCI SSC), and this policy sets out how Canterbury City Council and its staff will comply with these standards. Failure by the council to comply with the standards could result in regular and large fines and also no longer being permitted to process card payments.

It is important that all card processing activities are conducted in accordance with this policy and no activity may be conducted, nor technology employed, that might obstruct compliance with any part of this policy.

There are 12 broad areas, grouped by 6 headings, covered by the security standards, some of which affect how ICT, system suppliers or system administrators will set up the council's systems and others that impact directly on staff throughout the council who take card payments from customers. The 12 areas, and the 6 grouped headings, are:

Build and maintain a secure network and systems:

- Install and maintain a firewall configuration to protect cardholder data;
- Do not use vendor-supplied defaults for system passwords and other security parameters;

Protect cardholder data:

- Protect stored cardholder data;
- Encrypt transmission of cardholder data across open, public networks;

Maintain a vulnerability management program:

- Protect all systems against malware and regularly update anti-virus software or programs;
- Develop and maintain secure systems and applications;

Implement strong access control measures:

- Restrict access to cardholder data by business need to know;
- Identify and authenticate access to system components;
- Restrict physical access to cardholder data;

Regularly monitor and test networks:

- Track and monitor all access to network resources and cardholder data;
- Regularly test security systems and processes;

Maintain an information security policy:

- Maintain a policy that addresses information security for all personnel.

This policy lays down the guidelines by which we will achieve compliance against these standards. Where possible, risk will be managed and requirements on the council will be reduced by the use of appropriate payment channels or alternative suppliers. However, an assessment will be made for each payment channel individually.

2. Statement of Applicability

PCI DSS compliance for each authority is the responsibility of the PCI Compliance Officer.

The policy applies primarily to any staff member, but also extends to contractors of the council, suppliers, hosts of external systems and anyone else who is involved in processing card payments, handling of till receipts, or with responsibility for payment systems or networks, even on a temporary basis. However, not all parts of the policy apply to all staff, so the requirements are broken down into the different user groups. Recognised user groups are:

- Staff processing card payments. This could be face to face payments, or payments taken over the phone, and processing card refunds, and includes contractors or anyone else used to process card payments directly for the council.
- Staff who have interactions with card processing companies and/or banks for the purposes of financial reconciliation, including contractors or anyone else employed by the council to carry out this work.
- System administrators. This covers any system that has a card payment element, including till systems in use at various outlets within the district.
- ICT staff, with regard to systems connected to, or using, the council network.
- Suppliers of hosted systems have the same responsibilities as ICT for any systems that are hosted externally and not on the council network.
- PCI Compliance Officer.
- All staff. There are a few requirements that all staff should be aware of, as it affects the handling of till receipts, or considerations when visitors are in the office.

Staff within these groups will need to work together to achieve and maintain PCI DSS compliance. Technical advice will be provided by the most appropriate people, but any changes or introduction of new systems or processes should ultimately be signed off by the PCI Compliance Officer, as the system will need to comply with PCI DSS requirements.

If any person is found to have breached this policy, they will be subject to the council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of offenders.

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or the PCI Compliance Officer.

Identified Roles

It is recognised that each council has different job titles, so the following table is provided to help staff identify who they should contact, and also so that individual staff are aware of their responsibilities.

	Canterbury	Dover	Thanet
PCI Compliance Officer	Claire Stanbury		
ICT	EKS ICT Team	EKS ICT Team	EKS ICT Team
Corporate Information Officer	Matthew Archer		
Corporate Governance and Risk Officer	Sue Wallis		
Customer Service Manager	Jo Read	Jo Read	Jo Read
Office Services Manager	Alexis Jobson		

3. Definitions

PCI DSS is concerned with account data for debit and credit cards. Account data is made up of cardholder data and sensitive authentication data (also known as sensitive information), and there are specific rules around the use, storage and transmission of these two types of data.

What is Cardholder Data?

Cardholder data refers to the card number across the centre of the card (otherwise known as the Primary Account Number, or PAN), the cardholder name, the expiry date and the service code (also known as the security code).

The primary account number is the defining factor for cardholder data. If the cardholder name, service code, and/or expiry date are stored, processed or transmitted with the PAN, they must be protected in accordance with the PCI DSS requirements. Storage of cardholder data is permitted, but the PAN must always be rendered unreadable.

What is Sensitive Information?

Sensitive information is security-related information. This includes (but is not limited to) card validation codes, full track data (from the magnetic stripe or equivalent on a chip), PINs and PIN blocks. This information is used to authenticate cardholders and/or authorise payment card transactions.

Under no circumstances can sensitive information be stored in any form.

4. Approach to PCI DSS Compliance

Full compliance to the highest level of requirements is very resource intensive. Where possible, we will look to use systems and processes that reduce the level of compliance required. For this reason it is important to consult the PCI Compliance Officer before starting any process re-design, and particularly any procurement process, involving card payments. It is also important to think about the visibility of cardholder data during the processing of the payment, so the PCI Compliance Officer should also be consulted regarding office moves.

The requirements set out below are based on the full PCI DSS requirements. Implementing systems and processes that reduce the compliance level required will mean that the requirement could be not applicable to all channels. However, they are included in the policy document so that we have an agreed process to follow should any channel be identified as being of the highest compliance level.

In order to remove the requirement for the highest levels of control, we need to ensure that systems are not stored on our network, and that payments are not processed on devices that are connected to our network unless they have validated point to point encryption.

5. Requirements

5.1 Firewall

Why is this important?

Often, seemingly insignificant paths to and from external networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

A firewall examines network traffic and blocks the transmissions that do not meet the security criteria.

Responsibilities of PCI Compliance Officer

5.1.1 To ensure that policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.

Responsibilities of ICT

5.1.2 To ensure that policies and operational procedures are in place for managing firewalls, and that these are complied with.

5.1.3 To maintain firewall and router configuration standards in line with up-to-date PCI DSS requirements, and to review the rule sets at least every six months.

5.1.4 To ensure the firewall configuration will restrict connections between untrusted networks and any system components in the cardholder data environment. Inbound and outbound traffic will be restricted to just what is necessary

5.1.5 To prohibit direct public access between the internet and any system component in the cardholder data environment.

5.1.6 If we have any environments that require the highest level of control, to install firewall software on any corporate mobile devices provided that connect to the internet when outside the network, and which are also used to access the network.

Responsibilities of all staff

5.1.7 To ensure that any devices that connect to the internet when outside the network are not connected to any networked equipment without being scanned by ICT, unless approved firewall and anti-virus software has been installed.

5.2 System passwords and security parameters

Why is this important?

Malicious individuals often use vendor default passwords and other default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information. Default passwords and settings must be changed in order to protect against this threat.

Responsibilities of PCI Compliance Officer

5.2.1 To ensure that policies and procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.

5.2.2 To ensure that inventories of system components exist for all payment areas and that procedures are in place for these to be checked daily.

5.2.3 To maintain a record of systems that are not up to date, and the risk assessments completed, reviewing these at least six-monthly to understand the current risk and to review if the issue still exists.

Responsibilities of ICT

5.2.4 To ensure that all systems installed on the network have default passwords changed before installation on the network.

5.2.5 To develop configuration standards for all system components to address all known security vulnerabilities and that are consistent with industry accepted ICT risk management standards.

5.2.6 When implementing upgrades or new software into the cardholder environment, to seek advice from the software vendor about relevant security vulnerabilities, and how the software should be configured in order to fix or minimise the vulnerabilities where feasible.

5.2.7 To complete a risk assessment if it is not feasible to install latest patches; which must be sent to the PCI Compliance Officer.

Responsibilities of system administrators

5.2.8 To ensure that all systems installed on the network have all default passwords changed, working with ICT support if necessary.

5.2.9 To maintain an inventory of system components for payment systems/point of sale terminals.

5.2.10 To ensure that processes are in place for daily checks of system components, comparing equipment in place to that shown in the inventory, and that these are carried out each day.

Responsibilities of staff on point of sales terminals

5.2.11 To check at the start of each day that the components shown in the inventory are in place and have not been compromised, completing the daily sign off sheet to confirm that all components have been checked and are in order.

5.3 Protecting stored cardholder data

Why is this important?

Cardholder data must be protected to prevent theft or misuse of this information, which could lead to fraudulent transactions being processed. This includes any information held electronically or on paper records, and information being sent between staff. By ensuring that the amount of data held is minimal, or masked so that it cannot be read, the risk is reduced.

Responsibilities of PCI Compliance Officer

5.3.1 To ensure that policies and procedures for protecting cardholder data are documented, in use, and known to all affected parties.

Responsibilities of ICT

5.3.2 To ensure that no logs, history or trace files store sensitive information or unmasked cardholder data.

5.3.3 To apply processes that actively search for sensitive information or unmasked cardholder data every six months.

Responsibilities of system administrators

5.3.4 To ensure that payment systems never store sensitive information, including the card security code, after a payment has been authorised.

5.3.5 To ensure that the full PAN is masked when displayed on screens, receipts, printouts etc. The first six and last four digits are the maximum number of digits that can be displayed.

5.3.6 To ensure that the maximum amount of information recorded and stored is the card number (rendered unreadable), expiry date and name. This applies to printed till receipts, as well as electronic information stored.

Responsibilities of managers

5.3.7 To ensure that departmental retention schedules include cardholder data, whether in electronic systems or on till receipts, to ensure this is not stored any longer than necessary, and is destroyed securely. This information should only be stored for as long as is required for business, legal or regulatory purposes. Advice can be sought from the PCI Compliance Officer or the Corporate Information Officer if necessary.

5.3.8 To seek approval from the PCI Compliance Officer if data is to be held for longer than 18 months.

Responsibilities of staff processing card payments

5.3.9 To ensure that cardholder data, including the card security code, is never written down, and that it is never stored unencrypted after a payment has been authorised.

5.3.10 No cardholder data should ever be taken or stored off council premises.

5.3.11 To ensure that card numbers and security codes are not repeated in full back to customers in an area that can be overheard by others.

5.4 Encrypting transmissions of cardholder data

Why is this important?

Sensitive information must be encrypted during transmission to protect it from malicious individuals able to intercept the transmission. Misconfigured networks and vulnerabilities in security protocols continue to be targeted by malicious individuals to gain access to cardholder data and sensitive information.

Responsibilities of PCI Compliance Officer

5.4.1 To ensure that policies and procedures for encrypting transmissions are documented, in use, and known to all affected parties.

Responsibilities of ICT

5.4.2 To ensure that cardholder data is encrypted using strong cryptography and security protocols when being transmitted over open, public networks.

Responsibilities of staff processing card payments

5.4.3 To ensure that card numbers are never sent in emails, instant messaging, chat, or any other end-user messaging. This includes card numbers captured as part of a screen dump.

5.5 Anti-virus software and protection against malware

Why is this important?

Malicious software can enter the network during normal business activities, including email and use of the internet. This software can then be used to gain access to our systems and data in various ways. Anti-virus software must therefore be installed on all systems at risk of being affected, and on all hardware such as laptops and PCs.

General

The requirements within section 5.5 only apply if we have environments that require the highest levels of control. However, the installation, updating and use of anti-virus software would still be considered best practice and as such these requirements should be met as far as is possible.

Responsibilities of PCI Compliance Officer

5.2.12 To ensure that policies and procedures for protecting systems against malware are documented, in use, and known to all affected parties.

Responsibilities of ICT

5.2.13 To ensure that anti-virus software is installed on all systems at risk of being affected by malicious software. The software must be capable of detecting, removing and protecting against all known types of malicious software.

5.2.14 To ensure that anti-virus software in use is kept current and actively running, performs periodic scans and generates audit logs.

5.2.15 To ensure that anti-virus software cannot be disabled or altered by users, unless specifically authorised by management for a limited time period.

Responsibilities of staff processing card payments

5.2.16 To ensure that anti-virus software installed on hardware is actively running.

4.2 Develop and maintain secure systems

Why is this important?

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided patches, which must be installed promptly, to protect against the exploitation and compromise of cardholder data by malicious individuals.

General

5.6.1 As much as possible, we will limit exposure to these risks by using industry standard, PCI DSS compliant certified software and systems, rather than creating bespoke systems.

5.6.2 Most of the requirements within section 5.6 only apply if we have environments that require the highest levels of control. All responsibilities of the PCI Compliance Officer need to be met regardless, as do points 5.6.7, 5.6.9, 5.6.12, 5.6.13 and 5.6.15 to 5.6.17.

Responsibilities of the PCI Compliance Officer

5.6.3 To ensure that policies and procedures for developing and maintaining secure systems are documented, in place, and known to all affected parties.

5.6.4 To ensure that vulnerabilities identified through PCI compliance testing are addressed as they are discovered.

5.6.5 To provide testing card details to departments for testing payment systems and mechanisms.

5.6.6 To ensure that Open Web Application Security Project (OWASP) guidelines cover the requirements of PCI DSS.

Responsibilities of ICT

5.6.7 To employ a process to identify security vulnerabilities, and to assign a risk ranking to any newly discovered vulnerabilities.

5.6.8 To inform the PCI Compliance Officer and the Corporate Governance and Risk Officer once a vulnerability has been identified, detailing the risk identified and to discuss plans for remediation.

5.6.9 To work with system administrators to ensure that system components and software are kept up to date with security patches. Critical security patches should be implemented within 30 days if possible. Where this is not possible, the PCI Compliance Officer and the Corporate Governance and Risk Officer should be informed, so that the risk can be recorded and action monitored.

5.6.10 To work with system administrators to ensure that vulnerabilities identified through PCI compliance testing are addressed as they are discovered.

5.6.11 To ensure that change control processes are followed for all changes to system components, ensuring that live card numbers are not used for testing or development purposes.

5.6.12 To ensure that any software or web applications developed internally are compliant with Open Web Application Security Project (OWASP). When applications are developed which require a link to a payment mechanism, it must be discussed with the PCI Compliance Officer and be compliant with PCI DSS standards.

5.6.13 If applications are developed internally, ensure that developers use secure coding techniques, and understand how sensitive information will be handled in transmission, storage and memory.

5.6.14 To ensure that an automated technical solution that detects and prevents web-based attacks (for example, a web application firewall) is maintained in front of any public-facing web applications that have contact with the cardholder data environment, or review public-facing web applications via application vulnerability security assessment tools annually and after any changes.

Responsibilities of system administrators

5.6.15 To employ a process to identify security vulnerabilities, and to assign a risk ranking to any newly discovered vulnerabilities.

5.6.16 To inform the PCI Compliance Officer and the Corporate Governance and Risk Officer once a vulnerability has been identified, detailing the risk identified and to discuss plans for remediation.

5.6.17 To work with ICT to ensure that system components and software are kept up to date with security patches. Critical security patches should be implemented within 30 days if possible. Where this is not possible, the PCI Compliance Officer and the Corporate Governance and Risk Officer should be informed, so that the risk can be recorded and action monitored.

5.6.18 To work with ICT to ensure that vulnerabilities identified through PCI compliance testing are addressed as they are discovered.

5.6.19 To ensure that change control processes are followed for all changes to system components, ensuring that live card numbers are not used for testing or development purposes.

5.7 Controlled access

Why is this important?

To protect cardholder data and sensitive information, access to it should be limited to only those people with a need to access it.

Responsibilities of PCI Compliance Officer

5.7.1 To ensure that policies and procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.

Responsibilities of system administrators

5.7.2 To only grant access to system components that deal with cardholder data, and to cardholder data itself, to those that need access for the purposes of their job.

5.7.3 To ensure that access to a system is only granted once authorised by the line manager, and once the user has acknowledged that they have read and understood this policy, and will comply with its content.

5.7.4 To maintain an audit trail of access authorisation and acknowledgement of the policy.

5.7.5 To ensure that payment systems automatically deny access to the parts of the system that process cardholder data, so that access has to be expressly given.

Responsibilities of staff processing card payments

5.7.6 To ensure that cardholder data is never copied, moved or stored onto local hard drives or removable media, such as memory sticks.

5.8 Identifying and authenticating system access

Why is this important?

All users of payment systems should be identifiable, so that any discrepancies can be investigated and traced. The identification should ideally be by means of a unique computer log in, but can also be achieved by other means, such as the use of cameras overlooking cashier terminals (although care should be taken that the cameras do not record cardholder data being entered).

Minimum password requirements

5.8.1 The following are the minimum password requirements as set out by the PCI DSS requirements.

- Minimum length of at least 7 characters.
- Contain both alphabetic and numeric characters.
- Must be changed at least once every 90 days.
- Must not be the same as any of the last 4 passwords.

Responsibilities of PCI Compliance Officer

5.8.2 To ensure that policies and procedures for identification and authentication are documented, in use, and known to all affected parties.

Responsibilities of ICT

5.8.3 To ensure that multi-factor authentication is in place for remote access to the network by employees, administrators and third parties.

5.8.4 To ensure that vendor accounts are managed so that they are only enabled when authorised, and that they have access appropriate to their role. Access will be monitored.

5.8.5 To ensure that computers and other devices issued by ICT are set to lock after 15 continuous minutes of inactivity.

Responsibilities of system administrators

5.8.6 To ensure that unique IDs are provided to individual users, unless other identification means exist, such as cameras recording the cashiering area.

5.8.7 To ensure that password security settings for all systems that process cardholder data comply with the minimum password requirements set out in 5.8.1 above.

5.8.8 To immediately revoke the user IDs for any users no longer requiring access.

5.8.9 To remove or disable inactive user accounts at least every 90 days (or ensure that the payment system carries this out automatically).

5.8.10 To ensure that users are locked out after no more than 6 unsuccessful attempts of logging into the system, with a minimum lockout time of 30 minutes, unless cleared by an administrator.

5.8.11 To ensure that user identity is verified before modifying any authentication credentials such as passwords.

5.8.12 To use unique passwords for first time use and upon reset of accounts, and to ensure these are set to change immediately after first use.

Responsibilities of staff processing card payments

5.8.13 To only log in to the Council's approved payment systems using only the ID provided by the system administrator.

5.8.14 To ensure that personal login details are kept safe and **never** shared with others, and that passwords are changed if there has been a risk of passwords being shared or known by others.

5.8.15 To ensure that passwords used comply with the minimum password requirements set out in 5.8.1 above.

5.8.16 To lock the computer whenever leaving the office, or lock other devices when not in use.

5.8.17 To not amend the lockout time on any device beyond that set by ICT when issued.

5.9 Physical access

Why is this important?

Any physical access to data, or systems that house cardholder data, provides the opportunity for individuals to access devices or data and to remove information, and should be appropriately restricted.

This applies to electronic data, but also any paper that may contain cardholder data, such as till receipts.

Responsibilities of the PCI Compliance Officer

5.9.1 To ensure that policies and procedures for restricting physical access are documented, in use, and known to all affected parties.

5.9.2 To ensure that appropriate controls are in place for physical areas where cardholder data is processed, to prevent reading of cardholder data by unauthorised persons.

Responsibilities of ICT

5.9.3 To ensure that electronic media is stored securely, and when removed this is performed in line with agreed procedures.

5.9.4 To store media backups in a secure location, and to review the location's security annually.

5.9.5 To ensure that cardholder data is rendered unrecoverable on any electronic media that is no longer required.

Responsibilities of system administrators

5.9.6 To protect devices that capture payment card data from tampering and substitution.

5.9.7 To maintain an up-to-date list of card payment devices, including the following:

- Make and model of device;
- Location of device;
- Serial number or other unique identification information;
- Device expiry date;
- Any substitution of device due to authorised replacement or repair.

5.9.8 To periodically inspect devices for tampering and substitution.

5.9.9 To train personnel to be aware of attempted tampering or replacement of devices.

Responsibilities of the Customer Service Manager

5.9.10 To ensure that all physical areas where cardholder data is processed are laid out and access is controlled in appropriate ways, to prevent reading of cardholder data by unauthorised persons.

5.9.11 To ensure that main reception maintain a log of visitors, including details of the visitor's name, firm represented if applicable, the person they are visiting and the date of the visit.

Responsibilities of the Office Services Manager

5.9.12 To ensure that arrangements exist for the secure destruction of paper based confidential information in such a way that the data cannot be reconstructed.

Responsibility of service managers

5.9.13 To ensure that remote sites have appropriate visitor logs and procedures in place, ensuring that visitors are recorded and can be identified whilst on site.

5.9.14 To ensure that all records, whether paper or electronic, which contain cardholder data are stored and transported securely, preferably by using corporate methods for the destruction of confidential information.

5.9.15 To ensure that records are clearly marked so that they can be identified as confidential before being transported. Where records are sent from one building to another, this must be done in a secure way that can be tracked, such as using the standard council courier service.

Responsibilities of all staff

5.9.16 To follow the standard council guidelines with regard to visitors, ensuring that they have signed in at reception, are authorised before entering areas where cardholder data is processed or maintained, that they wear the visitor badge issued at reception, and that the badge is given up at the end of their visit.

5.9.17 To ensure that paper records being sent to another area are sent in a non-transparent sealed envelope or wallet, and are not loose within a clear messenger bag or wallet.

5.9.18 To store till receipts or other cardholder data records in line with local policies, ensuring that they are secure at all times.

5.9.19 To ensure that till receipts or other records containing cardholder data are disposed of using the council's confidential waste bins, and that they are kept no longer than necessary, in line with departmental retention schedules.

5.10 Monitoring access to data

Why is this important?

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs allows thorough tracking, alerting and analysis if something should go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

General

5.10.1 The requirements within section 5.10 only apply if we have environments that require the highest levels of control. Where possible we will implement systems and processes that require lower levels of control. However, should systems be implemented that require the highest level, then the requirements within this section will need to be complied with.

Responsibilities of PCI Compliance Officer

5.10.2 To ensure that policies and procedures for monitoring access to network resources and cardholder data are documented, in use, and known to all affected parties.

Responsibilities of ICT

5.10.3 To maintain system logs that link all access to system components to individual users.

5.10.4 To use appropriate software to search for cardholder data on a quarterly basis.

5.10.5 Where cardholder data exists, to maintain logs that are able to reconstruct:

- access to cardholder data;
- actions taken when logged in with administrator privileges;
- access to audit trails;
- invalid login attempts;
- use of authentication mechanisms;
- initialisation, stopping, or pausing of audit logs;
- creation and deletion of system level objects.

5.10.6 To ensure that logs record the identity of the user, date and time of events, and whether or not events were successful.

5.10.7 To ensure that audit logs maintained are secure against alteration, and can only be viewed by those with a job related need.

5.10.8 To review logs and security events to identify anomalies or suspicious activity on a daily basis for all security events, system components that store, process or transmit cardholder data or sensitive information, all critical system component logs and logs of all server and system components that perform security functions.

5.10.9 To review logs of all other systems on an alert basis to identify anomalies or suspicious activity.

5.10.10 To ensure that logs are routinely backed up and maintained for 1 year.

5.10.11 To ensure that all system clocks and times are synchronised.

5.11 Testing security systems and processes

Why is this important?

Vulnerabilities are being discovered continually, and being introduced by new software. System components, processes, and custom software should be tested

frequently to ensure security controls continue to reflect a changing environment.

General

5.11.1 Most of the requirements within section 5.11 only apply if we have environments that require the highest levels of control. However, we will need to perform quarterly internal and external network scans regardless of the other controls required. All other requirements will only be needed where a system is implemented that requires the highest level of control.

Responsibilities of PCI Compliance Officer

5.11.2 To ensure that policies and procedures for security monitoring and testing are documented, in use, and known to all affected parties.

Responsibilities of ICT

5.11.3 To test quarterly for the presence of wireless access points, taking appropriate action to close any unauthorised points identified.

5.11.4 To maintain an inventory of authorised wireless access points.

5.11.5 To perform quarterly internal and external network scans to identify any PCI vulnerabilities.

5.11.6 To perform internal and external network scans to identify any PCI vulnerabilities after any significant changes in the network, and to rescan as needed until all high risk vulnerabilities are resolved. If an upgrade or modification could allow access to cardholder data, or affect the security of the cardholder data environment, this would be considered significant.

5.11.7 To undertake internal and external penetration testing annually, with extra scans taking place after any significant changes in infrastructure or relevant applications, and to rescan as needed until all high risk vulnerabilities are resolved.

5.12 Maintaining a policy for ourselves and contractors

Why is this important?

All personnel should be aware of the sensitivity of data, and their responsibilities for protecting it. A strong security policy sets the tone for the whole entity and informs personnel of what is expected of them.

When choosing suppliers to work with for payments, it's also necessary to ensure they are aware of the responsibility of protecting such data, and that their systems and processes are PCI DSS compliant.

Responsibilities of the PCI Compliance Officer

5.12.1 To maintain and review the PCI DSS policy annually, taking into account up-to-date PCI guidance.

5.12.2 To ensure that an annual audit of PCI compliance is carried out to ensure continued compliance with the standards, and look at newly identified risks.

5.12.3 To ensure that a risk assessment is carried out upon significant changes to the environment, such as the introduction of a new payment channel.

5.12.4 To maintain a list of third party companies who provide card payment services on behalf of the council, and ensure that these companies are also compliant with PCI standards.

5.12.5 To obtain an annual statement from suppliers providing card payment services, recognising their responsibility for the security of cardholder data they store, process or transmit on behalf of the council.

5.12.6 To ensure the maintenance of an incident response plan, ensuring that it contains all requirements as set out by the PCI council. As a minimum, this includes:

- Roles, responsibilities and communication strategies in the event of a compromise, including notification to payment brands.
- Specific incident response procedures.
- Business recovery and continuity procedures.
- Data backup processes.
- Analysis of legal requirements for reporting compromises.
- Coverage and responses of all critical system components.
- Reference or inclusion of incident response procedures from the payment brands.

5.12.7 To ensure that the Information Security Policy complies with up to date PCI DSS requirements.

5.12.8 To implement a formal security awareness program to make all personnel aware of the importance of cardholder data security, educating staff annually and upon hire.

Responsibilities of ICT

5.12.9 To assist in the annual audit of PCI compliance, providing information on how the networks and systems meet up-to-date PCI requirements.

Responsibilities of system administrators

5.12.10 To assist in the annual audit of PCI compliance, providing information as requested to prove that systems are still compliant with up-to-date PCI requirements.

5.12.11 If appointing a new company to handle card payments on our behalf, to ensure their PCI status is checked and taken into account before they are appointed. Guidance can be sought from the PCI Compliance Officer.

5.12.12 To ensure that any new contracts awarded for payment solutions require adherence to PCI DSS by the service provider and include acknowledgement of responsibility for the security of cardholder data.

Responsibilities of staff processing card payments

5.12.13 To ensure they are familiar with their responsibilities under this policy, and that they are being carried out fully.

Responsibilities of all staff

5.12.14 To ensure that any concern regarding a security risk or abuse of the system or policy is reported to the PCI Compliance Officer. If the matter is particularly sensitive it can be raised under the Council's whistle blowing policy.

Policy Compliance

If any person or organisation in scope is found to have breached this policy one of the following consequences may be followed;

- Councils' disciplinary procedure.
- Breach of contract.
- Member code of conduct.

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or Senior Information Risk Office.

Document Control		
Title/Version	-	CIGG Password Policy 1.0
Owner	-	Corporate Information Governance Group
Date Approved	-	
Review Date	-	
Reviewer	-	

Revision History			
Revision Date	**Reviewer (s)**	**Version**	**Description of Revision**
22/10/2015	Will Causton	1.0	Initial Version
19/01/2016	Hannah Lynch	1.1	Format Changes
23/09/2016	CIGG	1.2	Final Review

Business Continuity Policy

- **Introduction**
- **Scope**
- **The Policy**
  - Background
  - Key Messages
  - Risks
  - Policy Detail
  - Responsibilities

- **Policy Compliance**
  - Document Control

Introduction

This policy forms part of the Corporate Information Governance Group policy framework. It supercedes all previous policies on this subject matter.

Scope

This Policy applies to, but is not limited to, all of the councils, Councillors, Employees, Partners, contractual third parties and agents of the councils.

Business Continuity Policy

Background

A disaster which prohibits access to the councils premises or severely reduces the available staff would affect critical business procedures, the consequences of which can be severe and include substantial financial loss, an inability to achieve levels of service, embarrassment and loss of credibility or goodwill for the organisation. The consequential damage can have a much wider impact on staff welfare and the general public. The benefit therefore of having a recovery plan that can be implemented with the minimum of delay, will significantly reduce not only the level of disruption, but also the cost of recovering from the disruption, including reducing the cost of reduced productivity to the council, and should ensure the continued confidentiality, integrity and availability of information.

Key Messages

The aim of this policy is to ensure that all information held by the council can be reinstated as soon as possible, ensuring an unbroken level of frontline services, whilst full restoration is planned for and implemented.

The objectives of business continuity planning are to ensure that the council:-

- Understands its critical activities and maintains the capability to resume operations within agreed timeframes, following the deployment of a contingency planning response;
- Increases resilience by protecting critical information assets (electronic and otherwise) through a co-ordinated approach to management and recovery; and
- Minimises impacts using a focused, well-managed response activity.

Risks

- Business and Efficiency
- The Freedom of Information Act
- Data Protection Act/ Subject Access Requests
- Reputational Damage
- Financial Penalties
- Integrity of information

Policy Detail

The council's policy is to maintain the continuity of its activities, systems, facilities and processes and where these are disrupted by any event to enable it to return to 'normal' operations as soon as possible, taking fully into account the impact of any delay on the council's quality of service, reputation, finances and integrity of information held.

This policy is intended to ensure:

- The concept of Business Continuity and the council's policy and approach is understood by all stakeholders;
- Internal and external dependencies on information in respect of, customers, suppliers, partners and resource implications are identified;
- Individual service business continuity plans are developed to ensure the integrity and future recovery of information in the event of an interruption to services;
- Plans are systematically maintained and tested; and
- a programme of training and communication is put in place.

The Policy assumes a worst-case scenario in which critical information systems and resources are destroyed by fire, other natural events, or by unauthorised entrants committing acts of destruction, theft or sabotage that prevent key service delivery functions being undertaken.

It is assumed that the council's policy as it applies to records management, file management, computer security in general and virus protection in particular, is being applied. Similarly, it also assumes that fire prevention, physical security and health and safety at work standards are also being applied. It assumes that inventories of hardware/software, other business systems and major items of equipment are maintained by Divisions.

Responsibilities

The council should maintain a Business Continuity Plan which includes the responsibility for the continued integrity and safeguarding of the information during the recovery process.

- **Corporate Information Governance Group**

To advise each authority's SIRO, to review the elements of the BCP in respect of information integrity and retrieval for each authority, to effectively manage information and security risks and to monitor and report via the SIROs any security breaches.

- **Senior Information Risk Owner**

The SIRO implements and leads the Information Governance (IG) risk assessment and management processes within the Organisation and advises on the effectiveness of information risk management across the Organisation.

- **Information Asset Owners**

The Information Asset Owner, who should be a system user of appropriate seniority, must ensure that:-

1. BCP controls are in place, which are appropriate to the sensitivity of the information held.

2. The major risks which may threaten the confidentiality, integrity and availability of the information are identified and, where possible, mitigated;

3. The integrity of information is maintained during a BCP event.

Policy Compliance

If any person or organisation in scope is found to have breached this policy one of the following consequences may be followed:-

- Councils' disciplinary procedure.
- Breach of contract.
- Member code of conduct.

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or Senior Information Risk Officer.

Document Control		
Title/Version	-	Business Continuity Policy
Owner	-	Corporate Information Governance Group
Date Approved	-	
Review Date	-	
Reviewer	-	CIGG

Revision History			
Revision Date	**Reviewer (s)**	**Version**	**Description of Revision**
22/10/2015	Dave Randall Colin Cook	1.0	First Draft for Consideration
23/09/2016	CIGG	1.1	Final Review

Information Risk Management Policy

Contents:

- **Introduction**
- **Scope**
- **The Policy**
  - Background
  - Key Messages
  - Risks
  - Policy Detail
  - Responsibilities
- **Policy Compliance**
  - Document Control

Introduction

This policy forms part of the Corporate Information Governance Group policy framework. It supersedes all previous policy on this subject matter.

Information risk management is an essential element of broader information governance and is an integral part of good management practice. It is inherent in all administrative and business activities and all staff are responsible for continuously managing information risk. Information risk management should therefore be embedded into business processes and functions.

It should be noted that this policy complements and applies to the working of the council's Risk Management Strategy, and does not supersede it.

Scope

This Policy applies to, but is not limited to, all of the councils, Councillors, Employees, Partners, contractual third parties and agents of the councils.

Information Risk Management Policy

Background

The council needs to collect and use certain types of information about its staff, residents, customers and clients in order to carry out its functions, but in doing so needs to ensure that it does this in accordance with the requirements of the Data Protection Act 1998.

The council therefore needs to have a framework to ensure that when new processes, services, systems and other information assets are introduced that the implementation conforms with; Confidentiality, Integrity and Availability (CIA) principles:

Confidentiality: Keeping information safe and secure.

- The privacy and security of information must be maintained. Only those with an legitimate need can access the information and those whose data we are protecting can have confidence in how we safeguard the information.

Integrity: Ensuring information remains accurate and unaltered.

- Having confidence that the information we have is accurate, up to date and free from corruption. This underpins effective decision making and business efficiency.

Availability: Ensuring the information is available to be accessed by authorised users.

- Information must be available to those authorised users at the time and place they need it, so they can effectively make decisions and perform their duties.

This framework sets out a mechanism and behaviours to ensure that information security is properly considered and that any known risks are identified and addressed.

Key Messages

The purpose of this Information Risk Management Policy is to;

- Assist in safeguarding the council's information assets.
- Protect the council, its staff and its customers from information risks where the likelihood of occurrence and the consequences are significant.
- Provide a consistent risk management framework in which information risks will be identified, considered and addressed.
- Encourage pro-active rather than re-active risk management.
- Meet legal and statutory requirements.

Risks

The consequences of poor information risk management may result in;

- Reputational Damage
- Financial Penalties
- Damage to Integrity of information
- Loss of Business and Efficiency

Policy Detail

Documented Information Policies

The council has a number of documented information governance policies and these will be reviewed via the Corporate Information Governance Group on an ongoing basis. All changes to these policies should be formally disseminated to all staff.

Information Risk Register

Any identified information risks will be added included in the Corporate Risk Register which will include the departmental responsibility, the impact and likelihood of the risk, the owner of the risk and the actions being taken to mitigate the risk. Information risks will be captured in the following ways:

a) Risks identified through any procedural changes introduced.

b) Risks identified through formal projects.

c) Outcomes of internal data audits.

d) Risks identified and discussed at the Technical Steering Group.

e) Issues raised at the CIGG.

f) Issues identified by staff.

g) Information Incident management.

h) Any other ad-hoc issues identified by EKS ICT, council staff or customers.

a) Procedural Changes

When the council implements new or changed systems, procedures or contracts, or moves premises, these could affect the way information is stored, processed and shared. Where any changes are planned, it is important that risks to the security of information are recorded and monitored, that the risk is mitigated or accepted, and that a named individual is responsible for these decisions.

All ICT or new system development must firstly be reviewed and approved by the corporate body that exists to oversee systems development. All new projects, including ICT or capital projects must prepare a risk register. Any new risks that are considered of such a nature that they may impact corporate information risks should be submitted to the Office of the SIRO, who will then review these and where appropriate arrange for an update to the Corporate Risk Register.

b) Project Risks

All key projects, including ICT or capital projects must prepare a risk register. Where these are ICT projects the Project Manager must ensure that risks identified through the project review process should be referred to the Office of the SIRO who will assess the risks and add them to the Corporate Risk Register where appropriate.

c) Data Audits/Internal Audits by EKAP

Each service area will undertake data audits in their service area to assess how their data is stored and processed, as well as to detail who has responsibility for the data held and how the data is being managed overall by that service. These data audits will identify areas of risk, and these risks will be assessed by the Office of the SIRO for inclusion in the Corporate Risk Register where appropriate.

d) Technical Steering Group

The Technical Steering Group (TSG) is responsible for the strategic and tactical approach to technology projects and programmes for the three East Kent Districts. This group consists of senior staff from each district as well as EKS ICT staff and is therefore aware of risks that may exist on a strategic and technical level. Where the TSG identifies risks it must ensure that these risks are referred to the Office of the SIRO who will assess the risk and record them on the Corporate Risk Register where appropriate.

e) Corporate Information Governance Group

The Corporate Information Governance Group (CIGG) is responsible for the strategic management and security of data held within the Council. This group consists of the SIROs and senior staff from each of the three East Kent Districts as well as EKS ICT staff and is therefore aware of the actual information breaches that have arisen and the potential risks that could arise in future. Where the CIGG identifies risks it must ensure that these risks are referred to the Office of the SIRO who will assess the risk and record them on the Corporate Risk Register where appropriate.

f) Risks identified by staff

It is often whilst staff are carrying out their normal duties that local or service risks are identified and these are often quite specific. Where such risks are identified these should be referred to the Office of the SIRO who will assess the risk and record them on the Corporate Risk Register where appropriate.

g) Information Security Incidents

All security incidents must be recorded on the council's ICT Information Security Incident Reporting System to ensure that it correctly reported and followed up.

g) Other ad hoc risks identified

All other appropriate issues that are identified by ICT, staff or customers should be referred to the Office of the SIRO who will assess the risk on a case by case basis and record them on the Corporate Risk Register where appropriate.

Review of Information Risks

The information risks included in the Corporate Risk Register will be reviewed six-monthly by the Corporate Management Team who will:

a) Qualify and state these risks so that these are clear.

b) Review the impact and likelihood of existing risks.

c) Agree actions to mitigate and address risks.

d) Undertake actions to address these risks.

e) Decide and Agree on the closure of risks.

Responsibilities

Senior Information Risk Owner

The SIRO implements and leads the Information Governance (IG) risk assessment and management processes within the Organisation and advises on the effectiveness of information risk management across the Organisation.

The (SIRO) is responsible for co-ordinating the development and maintenance of information risk management policies, procedures and standards for the Council. It is their role to:

- Ensure that the council's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.
- Oversee the development of this policy and a strategy for implementing the policy within the existing Risk Management and Information Governance Framework.
- Take ownership of risk assessment processes for information risk including the review of the process to support and inform the Governance Assurance Statement.
- Review and agree actions in respect of identified information risks.

- Provide a focal point for the resolution and/or discussion of information.

Information Asset Owners

Information Assets Owners (IAOs) will provide assurance that the information risk is being managed effectively for those information assets that they have been assigned ownership.

IAOs will be required to:

- Know what information comprises or is associated with the asset, and understand the nature and justification of information flows to and from the asset.

- Ensure the confidentiality, integrity, and availability of all information that their system processes and working with EKS ICT protect against any anticipated threats or hazards to the security or integrity of such information.

- Know who has access to the asset, whether system or information, and why, and ensures access is monitored and compliant with policy.

- Undertake information risk assessments on all information assets where they have been assigned ownership.

Staff

Everyone has a role in the effective management of information risk. All staff will actively participate in identifying potential information risks in their areas and contribute to the implementation of appropriate mitigating actions.

Policy Compliance

If any person or organisation in scope is found to have breached this policy one of the following consequences may be followed:-

- Councils' disciplinary procedure.
- Breach of contract.
- Member code of conduct.

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or Senior Information Risk Officer.

Document Control		
Title/Version	-	Information Risk Management Policy
Owner	-	Corporate Information Governance Group
Date Approved	-	
Review Date	-	
Reviewer	-	CIGG

Revision History			
Revision Date	**Reviewer (s)**	**Version**	**Description of Revision**
	Colin Cook	1.0	First Draft for Consideration
23/09/2016	CIGG	1.1	Final Review
29/09/2016	Timo Bayford	1.2	CIA definitions added to Background

Information Sharing Policy

- **Introduction**
- **Scope**
- **The Policy**
  - Key Messages
  - Policy Detail
  - Sharing Information
  - Information Sharing Agreements
  - Privacy Impact Assessment
  - Further Advice

- **Policy Compliance**
  - Document Control

Appendix1 -

Appendix 2 -

Introduction

This policy forms part of the Corporate Information Governance Group policy framework. It supercedes all previous policies on this subject matter.

Scope

This Policy applies to, but is not limited to, all of the councils, Councillors, Employees, Partners, contractual third parties and agents of the councils.

Data Sharing Policy

Key Messages

Government policy places a strong emphasis on the need to share information across organisational and professional boundaries, in order to ensure effective co-ordination and integration of services.

The Government has also emphasised the importance of security and confidentiality in relation to personal information and has strengthened the legislation and guidance in this area in particular through the Data Protection Act 1998 and the Information Governance Assurance Programme.

It is important that we protect and safeguard person-identifiable information that it gathers, creates processes and discloses, in order to comply with the law and to provide assurance to the public.

The Data Protection Act places a duty on all employees to protect personal information they may come into contact with during the course of their work.

In May 2011, the Information Commissioner issued a data sharing code of practice specifying that “under the right circumstances, and for the right reasons, data sharing across and between organisations can play a crucial role in providing a better, more efficient service …. but…. rights under the Data Protection Act must be respected. Organisations that don’t understand what can and cannot be done legally are as likely to disadvantage their clients through excessive caution as they are by carelessness.”

Information can relate to staff (including temporary staff), members of the public, or any other identifiable individual, however stored. Information may be held on paper, CD/DVD, USB sticks, computer file or printout, laptops, palmtops, mobile phones, digital cameras or even heard by word of mouth. Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, and must not be stored on removable or mobile media unless it is encrypted. Other alternatives to removable media should be chosen when sharing personal information.

Policy Detail

The aim of this policy is to:

- Provide a framework to:

  - Enable the legitimate sharing of data between staff, departments and other agencies.
  - Provide information to deliver better services.
  - To prevent and detect crime.
  - Consider the controls needed for information sharing.
  - Ensure the expected standards are met (including that partners to information sharing are aware of the obligations of consent or how to take appropriate account of an individual's objection).

- Establish a mechanism for the exchange of information between council departments, and the councils and other organisations.

Sharing Information

This policy covers two main types of information sharing:

- Systematic, routine information sharing where the same data sets are shared between the same organisations for an established purpose; and

- Exceptional, one-off decisions to share information for any of a range of purposes.

Different approaches apply to these two types of information sharing and this policy reflects this. Some of the good practice recommendations that are relevant to systematic, routine information sharing are not applicable to one-off decisions about sharing.

Systematic information sharing - This will generally involve routine sharing of data sets between departments and/or organisations for an agreed purpose. It could also involve a group of departments and/or organisations making an arrangement to 'pool' their data for specific purposes.

Ad hoc or 'one-off' information sharing - much information sharing takes place in a pre-planned and routine way. As such, this should be governed by established rules and procedures. However, departments/staff may also decide, or be asked, to share information in situations which are not covered by any routine agreement. In some cases this may involve a decision about sharing being made in conditions of real urgency, for example in an emergency situation.

When deciding whether to enter into an arrangement to share personal data (either as a provider, a recipient or both), you should consider what is the sharing meant to achieve? There should be a clear objective, or set of objectives. Please use the checklist at appendix 1.

In all circumstances of information sharing, staff will ensure that:

- When information needs to be shared, sharing complies with the law, guidance and best practice.

- Only the minimum information necessary for the purpose will be shared and, if sharing with providers, will only be shared when the contract explicitly permits it.

- Individuals' rights will be respected, particularly confidentiality and security.

- Reviews of information sharing should be undertaken to ensure the information sharing is meeting the required objectives/purpose and is still fulfilling its obligations.

Information Sharing Agreements

Information sharing agreements – sometimes known as 'Information or data sharing protocols' – set out a common set of rules to be adopted by the various organisations involved in an information sharing operation.

These could well form part of a contract between organisations. It is good practice to have a data sharing agreement in place, and to review it regularly, particularly where information is to be shared on a large scale, or on a regular basis.

An information sharing agreement must, at least, document the following:

- The purpose, or purposes, of the sharing.
- The legal basis for sharing.
- The potential recipients or types of recipient and the circumstances in which they will have access.
- Who the data controller(s) is and any data processor(s).
- The data to be shared.
- Data quality – accuracy, relevance, usability.
- Data security.
- Retention of shared data.
- Individuals' rights – procedures for dealing with access requests, queries and complaints.
- Review of effectiveness/termination of the sharing agreement; and
- any particular obligations on all parties to the agreement, giving an assurance around the standards expected.
- Sanctions for failure to comply with the agreement or breaches by individual staff.

Privacy Impact Assessment

Before entering into any data sharing arrangement, it is good practice to carry out a privacy impact assessment. This will help to assess the benefits that the information sharing might bring to particular individuals or society more widely. It will also help to assess any risks or

potential negative effects, such as an erosion of personal privacy, or the likelihood of damage, distress or embarrassment being caused to individuals.

As well as harm to individuals, staff should consider potential harm to the organisation's reputation which may arise if information is shared inappropriately, or not shared when it should be. Further information on privacy impact assessments can be sought from the Information Commissioners website.

Further advice

With information sharing there will always be exceptional and difficult circumstances where advice may be needed. If you require assistance please contact your data Protection Officer or your legal team.

Further information can also be found in the ICO Data Sharing Code of Practice:

https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

Policy Compliance

If any person or organisation in scope is found to have breached this policy one of the following consequences may be followed:-

- Councils' disciplinary procedure.
- Breach of contract.
- Member code of conduct.

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or Senior Information Risk Officer.

Document Control		
Title/Version	-	Data Sharing Policy
Owner	-	Corporate Information Governance Group
Date Approved	-	
Review Date	-	
Reviewer	-	CIGG

Revision History			
Revision Date	**Reviewer (s)**	**Version**	**Description of Revision**
15/10/2015	Dave Randall Matthew Archer	1.0	First Draft for Consideration
23/09/2016	CIGG	1.1	Final Review

Appendix One

Checklist for Appendix Two:

You must work through the checklist below and record the required information and the decision on the form at appendix two, this will help you make a sound decision by requiring you to consider relevant factors.

Systematic Data Sharing:

Is the sharing justified – what is the sharing meant to achieve, what are the risks, is sharing proportionate to the issue and could the objective be achieved without sharing personal data?

Do you have the power to share – have you identified the relevant functions or powers, the nature of the information that you are being asked to share and any legal obligation (for example a statutory requirement or a court order)?

If you decide to share – what information needs to be shared, with whom and what security measures are in place to protect the information?

One Off Data Sharing:

Is the sharing justified – do you think you should share the information, what are the risks to the individual and to society, is an individual at risk of harm, do you need to consider an exemption in the DPA to share?

Do you have the power to share – have you identified the relevant functions or powers, the nature of the information that you are being asked to share and any legal obligation (for example a statutory requirement or a court order)?

If you decide to share? – what information needs to be shared, with whom and what security measures are in place to protect the information, ensure you give it to the right person

Full details can be found on the ICO Data Sharing checklist:

https://ico.org.uk/media/for-organisations/documents/1067/data_sharing_checklists.pdf

Appendix Two

Data Sharing Request Form	
Name of Organisation requesting shared data:	
Name and Position of person requesting data:	
Date of Request:	
Reference to Data Sharing Agreement (*if applicable)*	
Data Requested:	
Purpose:	

Could the objective be achieved without sharing the data or by anonymising it? *It is not appropriate to use personal data to plan service provision, for example, where this could be done with information that does not amount to personal data.*	**YES** **NO**
What information needs to be shared? *You should not share all the personal data you hold about someone if only certain data items are needed to achieve the objectives. The third Caldicott principle specifies "Use the minimum necessary personal confidential data ".*	
Who requires access to the shared personal data? *You should employ 'need to know' principles, meaning that when sharing both internally between departments and externally with other organisations individuals should only have access to your data if they need it to do their job, and that only relevant staff should have access to the data. This should also address any necessary restrictions on onward sharing of data with third parties.*	
When will it be shared? *Again, it is good practice to document this, for example setting out whether the sharing should be an on-going, routine process or whether it should only take place in response to particular events.*	
How will it be shared? *This involves addressing the security surrounding the transmission or accessing of the data and establishing common rules for its security.*	
How will you check the sharing is achieving its objectives? *You will need to judge whether it is still appropriate and confirm that the safeguards still match the risks.*	

How will individuals be made aware of the information sharing? *Consider what to tell the individuals concerned. Is their consent needed? Do they have an opportunity to object? How do you take account of their objections? How do you ensure the individual's rights are respected and can be exercised e.g. how can they access the information held once shared?*	
What risk to the individual and/or the organisation does the data sharing pose? *For example, is any individual likely to be damaged by it? Is any individual likely to object? Might it undermine individuals' trust in the organisations that keep records about them?*	
Date Required by:	

Submitted By	
Name:	
Job Title:	
Date:	

Decision By	
Decision *Reason for disclosure or non-disclosure:*	
Name:	
Job Title:	
Date:	

Admin	
Date Data Disclosed:	

Public Services Network Personal Commitment

- **Introduction**
- **Scope**
- **The Policy**
  - Background
  - Key Messages
  - Risks
  - Policy Detail
  - Responsibilities

- **Policy Compliance**
  - Document Control

Introduction

This policy forms part of the Corporate Information Governance Group policy framework. It supercedes all previous policy on this subject matter.

Scope

This Policy applies to, but is not limited to, all of the councils, Councillors, Employees, Partners, contractual third parties and agents of the councils.

Public Services Network Personal Commitment

Background

The Public Sector Network (PSN) is a secure private Wide-Area Network (WAN) which enables secure interactions between connected Local Authorities and organisations that sit on the pan-government secure network infrastructure.

Some council staff will be required to have access to the facilities operated on this network in order for them to carry out their business. This may include staff having access to a secure email facility (GCSX email) or the DWP's Customer Information System. All staff requiring access to the PSN network in any way will be required to read and understand this Acceptable Usage Policy (AUP) and accept the Personal Commitment Statement.

This policy and statement does not replace the council's existing acceptable usage, or any other, policies. It is a supplement to them.

Key Messages

All users of the PSN must be aware of the commitments and security measures surrounding the use of this network.

Risks

There are risks associated with users accessing and handling information in order to conduct official council business.

This policy aims to mitigate the following risks:

- A breach of the Code of Connection for the PSN
- Loss of restricted information and data
- Information and data security incidents

Non-compliance with this policy could have a significant effect on the efficient operation of the council and may result in financial loss and an inability to provide necessary services to our customers.

Policy Detail

Each PSN user must read, understand and verify they have read and accepted this policy.

For the avoidance of doubt, the security rules relating to secure email and information systems usage include:

1. I acknowledge that my use of the PSN may be monitored and/or recorded for lawful purposes.

2. I agree to be responsible for any use by me of the PSN using my unique user credentials (user ID and password, access token or other mechanism as provided) and email address;

3. Will not use a colleague's credentials to access the PSN and will equally ensure that my credentials are not shared and are protected against misuse;

4. Will protect such credentials at least to the same level of secrecy as the information they may be used to access, (in particular, I will not write down or share my password other than for the purposes of placing a secured copy in a secure location at my employer's premises);

5. Will not attempt to access any computer system that I have not been given explicit permission to access;

6. Will not attempt to access the PSN other than from IT equipment and systems and locations which have been explicitly authorised to use for this purpose;

7. Will not transmit information via the PSN that I know, suspect or have been advised is of a higher level of sensitivity than my PSN domain is designed to carry (e.g. Secret or Top Secret);

8. Will not transmit information via the PSN that I know or suspect to be unacceptable within the context and purpose for which it is being communicated;

9. Will not make false claims or denials relating to my use of the PSN (e.g. falsely denying that an e-mail had been sent or received);

10. Will protect any sensitive or not protectively marked material sent, received, stored or processed by me via the PSN to the same level as I would paper copies of similar material;

11. Will always check that the recipients of e-mail messages are correct so that potentially sensitive information is not accidentally released into the public domain;

12. Will not auto-forward email from my GCSx email account to any other non-GCSx email account;

13. Will not forward or disclose any sensitive material received via the PSN unless the recipient(s) can be trusted to handle the material securely according to its sensitivity and forwarding is via a suitably secure communication channel;

14. Will seek to prevent inadvertent disclosure of sensitive information by avoiding being overlooked when working, by taking care when printing information received via PSN (e.g. by using printers in secure locations or collecting printouts immediately they are printed, checking that there is no interleaving of printouts, etc.) and by carefully checking the distribution list for any material to be transmitted;

15. Will securely store or destroy any printed material;

16. Will not leave my computer unattended in such a state as to risk unauthorised disclosure of information sent or received via PSN - e.g. logging-off from the computer, activate a password-protected screensaver etc., so as to require a user logon for activation);

17. Where IT Services has implemented other measures to protect unauthorised viewing of information displayed on IT systems (such as an inactivity timeout that causes the screen to be blanked requiring a user logon for reactivation), then I will not attempt to disable such protection;

18. Will make myself familiar with the council's security policies, procedures and any special instructions that relate to PSN;

19. Will inform my manager immediately if I detect, suspect or witness an incident that may be a breach of security

20. Will not attempt to bypass or subvert system security controls or to use them for any purpose other than that intended;

21. Will not remove equipment or information from council premises without appropriate approval;

22. Will take precautions to protect all computer media and portable computers when carrying them outside my organisation's premises (e.g. leaving a laptop unattended or on display in a car such that it would encourage an opportunist theft);

23. Will not introduce viruses, Trojan horses or other malware into the system or PSN;

24. Will not disable anti-virus protection provided at my computer;

25. Will comply with the Data Protection Act 1998 and any other legal, statutory or contractual obligations that the council informs me are relevant; and

26. If I am about to leave the council, I will inform my manager prior to departure of any important information held in my account and manage my account in accordance with the council's email and records management policy.

Responsibilities and Personal Commitment Statement

I, accept that I have been granted the access rights to PSN. I understand and accept the rights which have been granted, I understand the business reasons for these access rights, and I understand that breach of them, and specifically any attempt to access services or assets that I am not authorised to access, may lead to disciplinary action and specific sanctions. I also accept and will abide by this policy and personal commitment statement. I understand that failure to comply with this agreement, or the commission of any information security breaches, may lead to the invocation of the council's disciplinary policy.

If any user is found to have breached this policy, they may be subject to the councils disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or IT Services.

Policy Compliance

If any person or organisation in scope is found to have breached this policy one of the following consequences may be followed;

- Councils' disciplinary procedure.
- Breach of contract
- Member code of conduct

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or Senior Information Risk Officer.

Document Control		
Title/Version	-	PSN Acceptable Usage Policy and Personal Commitment Statement 1.2
Owner	-	Corporate Information Governance Group
Date Approved	-	
Review Date	-	
Reviewer	-	CIGG

Revision History			
Revision Date	**Reviewer (s)**	**Version**	**Description of Revision**
18/06/2015	Will Causton	1.0	Initial Version
13/07/2015	Will Causton	1.1	Changes following ICT Consultation and review of GSCP.
11/ 09/2015	Will Causton	1.2	Formatting Changes
08/04/2016	Hannah Lynch	1.3	Formatting Changes
23/09/2016	CIGG	1.4	Final Review

Digital Security – Network Access and Availability

Contents:

- **Introduction**
- **Scope**
- **The Policy**
  - Background
  - Key Messages
  - Policy Detail
    - User Access
    - Device Access
    - Remote Access
    - Democratic Services Committee Application (ModGov)
  - Data Backup
  - Personal Cloud Storage
  - Variation from Policy
- **Policy Compliance**
  - Document Control

- **Appendix 1; Supplier Remote Access and Desktop Sharing**
- **Appendix 2; Access from Overseas**

Introduction

This policy forms part of the Corporate Information Governance Group policy framework. It supercedes all previous policies on this subject matter.

Scope

This Policy applies to, but is not limited to, all of the councils, Councillors, Employees, Partners, contractual third parties and agents of the councils.

Digital Security

Background

Protecting the council's digital information assets is key to delivering the council's digital strategy. A failure of confidentiality, integrity or availability could have a significant effect on the ability of the council to deliver its services via digital platforms. This policy sets out the minimum requirements for access to the council's digital resources.

Key Messages

Access to the council's digital resources is only permitted from authorised devices by authorised personnel.

Access to digital resources will be controlled and monitored.

User accounts must be protected by a password.

User devices are not backed up by ICT, users must take care to ensure that important data is held in locations that are backed up: No important data should solely be stored on a user device.

Where the principles in this policy cannot be met, the risk must be recorded in the ICT Risk Management and Accreditation Database (RMAD) and authorised by the appropriate SIRO.

Policy Detail – Network Access

User Access

Access to the network will be controlled and monitored. Individuals will be given a unique account with which they will be able to access resources on the network.

The principles of role based access will be applied so that users have an appropriate level of access according to their function.

All accounts that are able to logon to the network must be traceable to an authorised and accountable individual.

Where a business unit has SIRO & ICT approval to use a generic network account, the business unit manager will be responsible for maintaining a record of use to maintain this accountability. This use of Generic accounts should be recorded in the RMAD and controls reviewed periodically to ensure they are effective.

All changes to user accounts and user rights must be authorised and logged.

User accounts will be disabled when no longer required.

User access and activity logs will be reviewed for unauthorised use.

Device Access

Access to the council's digital resources will only be permitted from devices owned and managed by the councils. The device must be authenticated.

Remote Access

The councils operate several technologies for remote access;

- Terminal Services via SSL VPN (Citrix and Juniper)
- Email to smart devices (ActiveSync)

Access to these services is only permitted from council owned and managed devices.

User access to Terminal Services platforms (Citrix and Juniper) will be protected by second factor authentication.

The Device and the User must be authenticated to the service.

Democratic Services Committee Application (Mod Gov)

Access to the Modern Government App and Website is not restricted to council owned and managed devices. Access is permitted from approved devices by authenticated users.

Data Backup

The council's' digital resources, stored on servers managed by ICT, will be regularly backed up.

Backups and incremental and will be held for 120 days/increments.

Backup data will not be solely stored on the same site from which the backup was obtained.

A random sample of test restores will be undertaken each month to verify the integrity of backed up data.

User devices are not backed up by ICT, users must take care to ensure that important data is held in locations that are backed up: No important data should solely be stored on a user device.

Personal Cloud storage

Personal Cloud Storage accounts (from any vendor) should never be used to store council data or conduct council business.

Apple iCloud is inappropriate for holding council data and should not be used even where the apple ID is provided by the council.

Other Cloud storage, where provided or managed by ICT, may be used where the Information Asset Owner permits that usage for that data.

Note:

Staff are reminded that smart devices should never be used as the primary means of storing council data. Data on smart devices is not automatically backed up, so any unique data should be moved to network storage (personal and shared drives) at the first opportunity - sending the information to yourself in an email is the easiest way to do this, then transfer any attachments to the appropriate Folder on the network, then remove the original from your smart device storage.

Email that is received on a smart device comes from the network - draft messages created on the smart device are stored on the device until they are successfully sent.

Staff should take a similar approach to any personal data they may be storing on a smart device i.e. photos, ensuring they have a copy of their personal data at all times. Network storage must not be used for personal data.

Variation from policy

The councils accept that occasionally, for operational reasons, it is not always possible to adhere closely to this policy. Requests for exemption will be considered by affected SIROs and granted on the merits of an individual case. Exemptions (and associated mitigations) will be recorded in the ICT RMADS and reviewed by the CIGG.

Policy Compliance

If any person or organisation in scope is found to have breached this policy one of the following consequences may be followed;

- Councils' disciplinary procedure.
- Breach of contract.
- Member code of conduct.

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or Senior Information Risk Officer.

Document Control		
Title/Version	-	Incident Management Policy
Owner	-	Corporate Information Governance Group
Date Approved	-	
Review Date	-	
Reviewer	-	CIGG

Revision History			
Revision Date	**Reviewer (s)**	**Version**	**Description of Revision**
03/08/2016	Will Causton	1.0	Initial Version
23/09/2016	Will Causton/CIGG	1.1	Amended following CIGG Consultation
05/10/2016	Hannah Lynch	1.2	Final Formatting

Appendix 1 Supplier Remote Access and Desktop Sharing

In many cases, suppliers require remote access to provide contracted services.

The requirement for the councils to own and manage devices used to connect is relaxed for this purpose, however the supplier must demonstrate management of their staff and equipment to a comparable standard as set out in the device management standards and user access controls set out in part 2 of this policy.

Note: If suppliers request details of our device management standards, please refer them to this Government document and ask them to provide written assurance that they operate systems that meet these principles.

https://www.gov.uk/government/publications/end-user-devices-security-principles/end-user-devices-security-principles

EKS ICT will maintain an operational process for managing Supplier Remote Access. The process will ensure that whoever facilitates access (where this is not EKS ICT) will ensure that:

- The information asset owner or system administrator has authorised the access.
- The identity of the individual who was granted access is recorded.
- The services accessed are recorded.
- The session is authorised for no more than 24 hours.

Access for periods greater than 24 hours may be permitted to facilitate extensive upgrades or commissioned installation works. Extended access should be authorised for a set period by the EKS Technical Systems Manager (or their delegate) and noted in the ICT Risk Management and Accreditation Document Set (RMADS).

Remote access must take place from a country with adequate data protection legislation. (See Appendix 2)

Desktop Sharing with external Third Parties

For desktop sharing; where a user engages directly with a third party via direct remote assistance products (like GoTomeeting or Teamviewer), that allow remote viewing or control of a console (Desktop). The user is responsible for ensuring that:

- The remote access session is authorised by the information asset owner.
- Supervised.
- The supplier meets the minimum standards for device management.
- The access is logged via the ICT self-service portal so that a record is maintained.

Appendix 2: Access from overseas.

Guidance from the Cabinet office and the ICO indicate that not all countries have adequate data protection measures. Additionally, staff should recognise that in some foreign countries they should expect to undergo electronic surveillance. With that in mind remote access for any purpose should only be provided from safe locations.

The Data Protection Act says that:

Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The EEA countries are currently the EU countries plus Iceland, Liechtenstein and Norway:

Austria	Germany	Malta
Belgium	Greece	Netherlands
Bulgaria	Hungary	Norway
Croatia	Iceland	Poland
Cyprus	Ireland	Portugal
Czech Republic	Italy	Romania
Denmark	Latvia	Slovakia
Estonia	Liechtenstein	Slovenia
Finland	Lithuania	Spain
France	Luxembourg	Sweden
		United Kingdom

Certain countries have been deemed to offer an adequate level of protection for personal data. Currently, the following countries are considered as having adequate protection.

Andorra	Guernsey	New Zealand
Argentina	Isle of Man	Switzerland
Canada	Israel	Uruguay
Faroe Islands	Jersey	United States of America

Digital Security – Monitoring and Standards

Contents:

- **Introduction**
- **Scope**
- **The Policy**
  - Background
  - Key Messages
  - Policy Detail
    - Protective Monitoring
    - Software Standards and Patch Management
    - Device Management Standards
  - Variation from Policy
- **Policy Compliance**
  - Document Control

- **Appendix 1; Protective Monitoring Controls**

Introduction

This policy forms part of the Corporate Information Governance Group policy framework. It supercedes all previous policies on this subject matter.

Scope

This Policy applies to, but is not limited to, all of the councils, Councillors, Employees, Partners, contractual third parties and agents of the councils.

Digital Security

Background

Protecting the council's digital information assets is key to delivering the council's digital strategy. A failure of confidentiality, integrity or availability could have a significant effect on the ability of the council to deliver its services via digital platforms. This policy sets out the minimum requirements for access to the council's digital resources.

Key Messages

The latest version of the software/firmware will be installed as soon as practicable.

The data environment will be monitored and reported upon.

Devices in use by our organisation will adhere to configuration standards.

Where the principles in this policy cannot be met, the risk must be recorded in the ICT Risk Management and Accreditation Database (RMAD) and authorised by the appropriate SIRO.

Policy Detail

Protective Monitoring

Protective Monitoring is a set of processes utilising technology or manual process that need to be in place in order to oversee how ICT systems are used; assuring user accountability for the use of ICT facilities.

The goal of protective monitoring is to provide assurance that the confidentiality, integrity and availability of the council's digital resources are maintained and to meet the requirement of any compliance sets and legal obligations that pertain to these resources (eg PSN, PCI-DSS, DPA, Computer Misuse Act)

It is not practical to set out every item of protective monitoring in this section of the policy. EKS ICT will maintain operational procedures to achieve the following (as a minimum) and consider the event conditions and uses cases as set out in Appendix 3.

- Who, What, How and When the network was accessed.
- Password abuses.

- Email and Web traffic.
- Malware detection.
- Software, Firmware and Operating system patch levels
- Intrusion detection
- Data Leak detection

Protective Monitoring logs may be provided to external agencies.

Protective Monitoring logs must be maintained for 12 months.

Protective Monitoring logs must be protected against unauthorised changes.

PCI-DSS SAQ D - Requirement 10 (Track and monitor all access to network resources and cardholder data) will be considered

Software Standards and Patch Management.

This section of policy sets out the standards and requirements that will be adhered to in the operation of the council's Software and Infrastructure assets.

Every council owned and managed device that can receive a firmware update and/or software update that accesses the council's Digital resources is in scope.

Key Messages

- The latest version of the software/firmware will be installed as soon as practicable.
- Un-patchable software will not be used.
- The software environment will be monitored and reported upon.
- Where these principles cannot be met, the exemption must be recorded in the ICT RMADS and authorised.

Patch management refers to the process by which an organization installs patches, which are fixes or updates to computer programs, operating systems, or applications. Patch management is an important element in mitigating the significant security risks associated with software vulnerabilities.

From an operational perspective, updates fix known flaws and bugs and sometimes provide new functionality. When a software vulnerability is discovered, the software vendor may develop and distribute a security patch or work-around to mitigate the vulnerability. Any significant delays in finding or fixing software with critical vulnerabilities provides opportunity for persistent attackers to break through, gain control over the vulnerable machines, gain access to the sensitive data contained on the computer, destroy information on the computer, or use the computer as a launching point for additional attacks to other computers on the network.

Outdated and unsupported software is more vulnerable to attack and exploitation. The majority of vulnerabilities exploited by viruses are ones for which a fix is available from the software vendor.

The councils are responsible for the security and integrity of the network, servers and IT Infrastructure. As part of the overall approach to maintaining the security, confidentiality and integrity of the network, this policy sets out the standards, responsibilities and approach that the IT provider will adhere to in the maintenance of the software and firmware environment.

This policy applies to all hosts that are connected to the corporate network. This includes, but is not limited to, Servers, Workstations, Network Infrastructure, SANs, Firewalls. It is the responsibility of everyone to work together to ensure that systems and devices they operate and use are maintained in accordance with this policy.

The risks and difficulty associated with updating firmware warrant a different standard to that of Operating systems and Application standards. A failure during the updating of firmware can lead to catastrophic, permanent failure of that equipment. For these reasons, it is not required that Firmware is updated upon release of new firmware by the manufacturer. Firmware must be updated to the latest stable release during commissioning of that infrastructure. Thereafter, it is required that firmware is updated if a security vulnerability (CVSS 4.0 or greater) is discovered within a release or to add desired functionality.

Hosts or applications found to be in breach of this policy may be disconnected from the network or have measures applied that reduce the risk, for example disabling internet access or limiting onward access. These measures may restrict non business critical functionality (eg disabling internet access from the affected system).

The network will be scanned quarterly for vulnerabilities and those vulnerabilities reported to the relevant technical manager, information asset owner and organisation PCI DSS risk officer.

Critical vulnerabilities must be resolved within 14 days, important vulnerabilities within 30 days and all others within 60 days.

Where it is known that a vulnerability is being actively exploited then mitigating action (e.g. patch applied) should be taken immediately.

Where a patch or mitigation is not deployed (or available) within the timescales above then there must be alternative mitigating action, such as disabling or reducing access to the vulnerable service.

Device Management Standards.

The councils will ensure that all IT systems, software and services are appropriately configured to reduce the level of inherent vulnerability. In particular applications, services, processes and ports not required are disabled by default. Default passwords will be

changed. Configuration control of applications installed and administrative oversight of devices will be maintained.

Users are only allowed minimum desktop customization, and are not permitted to make changes to system configuration settings (such as Antivirus, network settings or Update management) or have rights to install extra software (Local Admin).

All changes will be recorded, managed and authorised.

All owned and managed devices must meet these criteria.

- The device should be encrypted to protect data at rest
- The boot process should be secured so that it cannot be modified by unauthorised software or personnel
- All capable devices must have the capability to detect, isolate and respond to malicious software.
- The device must have the capability to report security events to the appropriate enterprise audit and monitoring services. The user must be prevented from tampering with the reporting of events.
- The device is able to constrain the set of ports (physical and logical) and services exposed to untrusted networks and devices.
- The device must be capable of receiving policy based configuration from the management platform (e.g. Active Directory/MDM)

Note: If suppliers request details of our standards, please refer them to this Government document and ask them to provide written assurance that they operate systems that meet these principles.

https://www.gov.uk/government/publications/end-user-devices-security-principles/end-user-devices-security-principles

Variation from Policy

The councils accept that occasionally, for operational reasons, it is not always possible to adhere closely to this policy. Requests for exemption will be considered by affected SIROs and granted on the merits of an individual case. Exemptions (and associated mitigations) will be recorded in the ICT Risk Management and Accreditation Database (RMADS) and reviewed by the CIGG.

Policy Compliance

If any person or organisation in scope is found to have breached this policy one of the following consequences may be followed;

- Councils' disciplinary procedure.
- Breach of contract.
- Member code of conduct.

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or Senior Information Risk Officer.

Document Control		
Title/Version	-	Incident Management Policy
Owner	-	Corporate Information Governance Group
Date Approved	-	
Review Date	-	
Reviewer	-	CIGG

Revision History			
Revision Date	**Reviewer (s)**	**Version**	**Description of Revision**
03/08/2016	Will Causton	1.0	Initial Version
23/09/2016	Will Causton/CIGG	1.1	Amended following CIGG Consultation
05/10/2016	Hannah Lynch	1.2	Final Formatting

Appendix 1: Protective Monitoring Controls

The Public Sector Network Code of Connection states:

"You will collect and retain event data and undertake activities that will help you detect actual or potential security incidents. You must have a protective monitoring policy that describes the use cases you are aiming to detect, which can be used to define event data collection.

Your policy must include both detection of technical attacks as well as important abuses of business processes. These conditions do not describe any specific events to collect or incidents to detect. The requirement is that the business has thought about and documented its collection and analysis requirements and that this has led to your approach to protective monitoring and intrusion detection."

The councils want to identify:

- Who? What? How? and When the network was accessed.
- Abuses of the Password policy.
- Abuses of Email and Web traffic.
- Malware Activity
- Software, Firmware and Operating system patch levels
- Intrusion detection
- Data Leak detection
- The use of unauthorised devices to access the council's Digital resources.

To achieve these aims, combinations of the following protective monitoring controls will be used.

Accurate Time in Logs

All devices shall use a common time source so that logs may be correlated. Internal time servers will use ntp.gcsx.gov.uk as their source.

Traffic Crossing a Boundary

Boundary firewalls will report connection details to the Syslog service.

Suspicious Activity at the Boundary

IDS and IPS will be operated at the boundary, logs will maintained within the IDS/IPS system. Critical events will be alerted in real time to the NOC Console.

Internal Workstation, Server or Device Status

Logs will be maintained of when hosts connected and for how long they were connected.

Logs will be maintained of USB devices connected or disconnected to a device.

Suspicious Internal Activity

User logon records will be reviewed for suspicious behaviour.

Password logs will be reviewed and challenged daily.

Changes to privileged active directory groups alerted in real time to the NOC Console

Network Connections

Network infrastructure will report 802.1x events to the syslog service; unknown devices will be alerted in real time to the NOC Console.

Session Activity by User and Workstation

Logon/logoff for machine and user accounts will be recorded in multiple locations, including, Active Directory Event log and AD Audit+ SIEM system.

Backup Status

The status of backup events will be alerted to the backup console and reviewed daily.

Email and Web traffic.

Web traffic from the corporate network will be logged.

Metadata (Sender, Recipient, Date, Time, Subject line and file name of any attachment) will be logged.

Management reports produced monthly

Malware detection and Data Leak detection

All malware and data leak events will be logged.

The Malware Detection console will be checked daily that the estate is able to update.

Malware detection events will be reported in real time to the service desk console.

Data leak detection events will be reported in real time to the NOC Console

The data leak prevention feature will alert on the following information patterns

- National Insurance Numbers
- Credit or Debit Card numbers.
- Bank account numbers
- The word “password”

Software, Firmware and Operating system patch levels.

A vulnerability scanning tool (Nessus) will be used to conduct a credentialed vulnerability scan quarterly.

Solar Winds Patch Manager (for Third party applications) and Microsoft Windows Update services will maintain logs of updates that have been installed and used to produce management reports about the status of patch levels.

Smart Devices

The configuration and location of Smart Devices will be monitored by the MDM platform.

Data Protection Policy

- **Contents**
- **The Policy**
  - The Policy Statement
  - About this Policy
  - Definition of Data Protection Terms
  - Responsibilities
  - Data Protection Principles
  - Fair and Lawful Processing
  - Processing for Limited Purposes
  - Notifying Data Subjects
  - Adequate, Relevant and Non-Excessive Processing
  - Accurate Data
  - Timely Processing
  - Processing in line with Data Subjects Rights
  - Data Security
  - Transferring Personal Data outside EEA
  - Disclosure and Sharing of Personal Information
  - Dealing with Subject Access Rights
  - Policy Changes
- **Schedule**
- **Policy Compliance**
  - Document Control

CONTENTS

CLAUSE

1. Policy statement....1
2. About this policy....1
3. Definition of data protection terms....1
4. Data protection principles....2
5. Fair and lawful processing....3
6. Processing for limited purposes....3
7. Notifying data subjects....3
8. Adequate, relevant and non-excessive processing....4
9. Accurate data....4
10. Timely processing....4
11. Processing in line with data subject's rights....4
12. Data security....5
13. Transferring personal data to a country outside the EEA....5
14. Disclosure and sharing of personal information....6
15. Dealing with subject access requests....7
16. Changes to this policy....7

SCHEDULE

SCHEDULE DATA PROCESSING ACTIVITIES....8

Data Protection Policy

1. POLICY STATEMENT

1.1 Everyone has rights with regard to the way in which their personal data in handled. During the course of our activities we will collect, store and process personal data about our customers, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

1.2 Data users are obliged to comply with this policy when processing personal data on our behalf. A serious breach of this policy may result in disciplinary action.

2. ABOUT THIS POLICY

2.1 This Policy will apply to all council employees working for Canterbury City Council, Dover District Council, Thanet District Council and employees of East Kent Services and the East Kent Audit Partnership. Hereafter they will be referred to collectively as 'the councils'. It also applies to the Councillors in each of the three districts.

2.2 The types of personal data that the councils may be required to handle include information about current, past and prospective customers and others that we communicate with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations.

2.3 This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.4 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.5 This policy has been approved by the Corporate Information Governance Group [CIGG], acting on behalf of the councils. It sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

2.6 The Data Protection Compliance Manager is responsible for ensuring compliance with the Act and with this policy. That post is held by the Senior Information Risk Owner, or their Deputy in each of the three councils.

Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Compliance Manager.

2.7 The designated officer will be responsible for completing the annual notification to the ICO and advising them of any updates to the register within 28 days.

3. DEFINITION OF DATA PROTECTION TERMS

3.1 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2 **Data subjects** for the purpose of this policy include all living individuals about whom we holds personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

3.3 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

3.4 **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our business for our own commercial purposes.

3.5 **Data users** are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

3.6 **Data processors** include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on the council's behalf.

3.7 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.8 **Sensitive personal data** includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

3.9 **Third Party** - Any individual/organisation other than the data subject, the data controller (the council's) or its agents.

3.10 **Relevant Filing System** - Any paper filing system or other manual filing system which is structured so that information about an individual is readily accessible.

4. RESPONSIBILITIES UNDER THE DATA PROTECTION ACT

Each council is a data controller under the Act.

The Data Protection Compliance Manager is responsible for ensuring compliance with the Act and with this policy and may assign officers to support this process.

The Corporate Management Team of each council is responsible for developing and encouraging good information handling practice within the council.

Compliance with data protection legislation is the responsibility of everybody who processes personal information.

The councils, through their staff are responsible for ensuring that any personal data supplied is accurate and up-to-date.

Councillors' Responsibilities

Members are regarded as Data Controllers in their own right if they process personal data either manually or by computer, whether on their own equipment or on equipment provided to them
by the Council.

There are three ways in which councillors might use personal data:

1. When considering issues and making decisions as part of the council's business – for example in committees or working groups. This is covered by the council's notification.

2. As a member of a political party canvassing for votes or working for a party. This is usually covered by the party's notification.

Councillors who are not a member of a political group must make their own arrangements to notify the ICO in order to process personal data in this way.

3. Carrying out casework. In this case the councillor is the data controller and is required to notify the ICO. It is the practice of the councils to notify the Information Commissioner's Office (ICO) on their behalf of all purposes for which the councillors hold and process personal data.

Where holding and proc**e**ssing personal data about individuals in the course of undertaking council business, a councillor will be covered by the council's notification to the ICO, and have the same responsibilities in respect of data protection as an employee of the authority.

5. DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

5.1 *Processed fairly and lawfully.*

The Act is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the Act. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met.

5.2 *Processed for limited purposes and in an appropriate way.*

In the course of our business, we may collect and process the personal data set out in the **Error! Reference source not found.**. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

We will only process personal data for the specific purposes set out in the **Error! Reference source not found.** or for any other purposes specifically permitted by the Act. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

5.3 ***Adequate, relevant and not excessive for the purpose.***

Information, which is not strictly necessary for the purpose for which it is obtained, should not be collected. If data are given or obtained which is excessive for the purpose, they should be immediately deleted or destroyed.

5.4 ***Accurate.***

Data, which are kept for a long time, must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that they are accurate. It is the responsibility of individuals to ensure that data held by the council are accurate and up-to-date. Individuals should notify the council of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the council to ensure that any notification regarding change of circumstances is noted and acted upon.

5.5 ***Not kept longer than necessary for the purpose.***

We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

5.6 ***Processed in line with data subjects' rights.***

We will process all personal data in line with data subjects' rights, in particular their right to:

- Request access to any data held about them by a data controller.
- Prevent the processing of their data for direct-marketing purposes.
- Ask to have inaccurate data amended.
- Prevent processing that is likely to cause damage or distress to themselves or anyone else.

We recognise that there is emerging case law on the rights of data subjects. We will review our policy and working practices in the light of this case law and at the same time seek to comply with the requirements of the new General Data Protection Regulations (GDPR).

5.7 ***Secure.***

See section headed ‘Data Security’.

5.8 ***Not transferred to people or organisations situated in countries without adequate protection.***

We may transfer any personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

- The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.
- The data subject has given his consent.
- The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.
- The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.
- The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

Subject to the requirements in the clause above, personal data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. That staff maybe engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

6. NOTIFYING DATA SUBJECTS

6.1 If we collect personal data directly from data subjects, we will inform them about:

(a) The purpose or purposes for which we intend to process that personal data.

(b) The types of third parties, if any, with which we will share or to which we will disclose that personal data.

(c) The means, if any, with which data subjects can limit our use and disclosure of their personal data.

6.2 If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

6.3 We will also inform data subjects whose personal data we process that we are the data controller with regard to that data, [and who the Data Protection Compliance Manager is].

7. DATA SECURITY

7.1 We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

7.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

7.3 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) Confidentiality means that only people who are authorised to use the data can access it.

(b) Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the council's central computer system instead of individual PCs.

7.4 Security procedures include:

(a) Entry controls. Any stranger seen in entry-controlled areas should be reported.

(b) Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

(c) Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.

(d) Equipment. Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

8. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

8.1 Personal data may be shared within the three council's or with East Kent Services or the East Kent Audit Partnership as part of our collaborative working arrangements.

8.2 We may also disclose personal data we hold to third parties:

(a) In the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets.

(b) If we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.

8.3 If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

8.4 We may also share personal data we hold with selected third parties for the purposes set out in the **Error! Reference source not found.**.

9. DEALING WITH SUBJECT ACCESS REQUESTS

9.1 Data subjects must make a formal request for information we hold about them. This must be made in writing. Employees who receive a written request should forward it to the council's FOI officer.

9.2 When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

(a) We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

(b) We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

9.3 Our employees will refer a request to their line manager [or the Data Protection Compliance Manager] for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

9.4 Any individual who wishes to exercise this right should submit a written request for subject access, provide satisfactory proof of identity, sufficient information to enable the data to be located, and pay the designated fee where appropriate.

9.5 Subject to satisfactory completion of 9.4, the data controller should respond within 40 days, ensuring that all data provided protects the interests of third parties by deleting any reference to them. A copy of the response should be retained for use in case of challenge.

10. DISCLOSURE OF DATA

The council must ensure that personal data are not disclosed to unauthorised third parties which includes family members, friends, landlords, government bodies, and in certain circumstances, the Police. All staff and members should exercise caution when asked to disclose personal data held on another individual to a third party.

The important thing to bear in mind is whether or not disclosure of the information is relevant to, and necessary for, the conduct of the council's business. Best practice, however, would be to take the contact details of the person making the enquiry and pass them onto senior management or the Data Protection Officer for a decision on the release of the information.

This policy determines that personal data may be legitimately disclosed where one of the following conditions apply:

1. the individual has given their consent (eg a member of staff or a Service User has consented to the council corresponding with a named third party);
2. where the disclosure is in the legitimate interests of the authority (eg disclosure to staff - personal information can be disclosed to other council employees if it is clear that those members of staff require the information to enable them to perform their jobs);
3. where the authority is legally obliged to disclose the data (eg ethnic minority and disability monitoring);

The Act permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- to safeguard national security*;
- prevention or detection of crime including the apprehension or prosecution of offenders*;
- assessment or collection of tax duty*;
- discharge of regulatory functions (includes health, safety and welfare of persons at work)*;
- to prevent serious harm to a third party;
- to protect the vital interests of the individual, this refers to life and death situations.

* Requests must be supported by appropriate paperwork.

Unless consent has been obtained from the data subject, information should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally a statement from the data subject consenting to disclosure to the third party should accompany the request.

If in doubt, staff should seek advice from their Head of Department or The Council's Data Protection Officer.

11. DATA SHARING

Information shared with third party organisations should comply with the Data Sharing Policy which forms part of the suite of Information Security policies available on the council's intranet.

12. RETENTION AND DISPOSAL OF DATA

The council discourages the retention of personal data for longer than they are required. Personal data must be disposed of in a way that protects the rights and privacy of data subjects (eg, shredding, disposal as confidential waste, secure electronic deletion).

13. USE OF CCTV

The council's use of CCTV is regulated by the ICO Code of Practice, supplemented by local policy and guidance.

14. FREEDOM OF INFORMATION ACT 2000

The Freedom of Information Act 2000 (FOIA) allows public access to all types of information held by public authorities. Requests for personal information will be dealt with under the Data Protection Act. The FOIA will not disclose private and confidential information about individuals without taking into account the requirements of the Data Protection Act.

15. COMPLAINTS

The council's 'comments and complaints procedure' will be applied in the event of any complaints received about requests for access to information under the Act. Details can be found on each council's website.

16. POLICY REVIEW

This policy will be managed and reviewed annually by the Corporate Information Governance Group. Reviews will be subject to scrutiny and, from time to time, updates and re-issues will be circulated.

However, the policy will be reviewed sooner if a weakness in the policy is highlighted, in the case of new risks, and/or changes in legislation.

17. FURTHER INFORMATION

For further guidance or advice on the Data Protection Act, please contact:

Canterbury: foi@canterbury.gov.uk, telephone 01227 862175.
Dover: Harvey.rudd@dover.gov.uk telephone 01304 872321.
Thanet:

Policy Compliance

If any person or organisation in scope is found to have breached this policy one of the following consequences may be followed:-

- Councils' disciplinary procedure.
- Breach of contract.
- Member code of conduct.

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or Senior Information Risk Officer.

Document Control		
Title/Version	-	Data Protection Policy
Owner	-	Corporate Information Governance Group
Date Approved	-	
Review Date	-	
Reviewer	-	CIGG

Revision History			
Revision Date	**Reviewer (s)**	**Version**	**Description of Revision**
05/08/2016	Matthew Archer	1.0	First Draft for Consideration
08/09/2016	Hannah Lynch	1.1	Formatting/ Amendments
23/09/2016	CIGG	1.2	Final Review

Appendix 4

End of Consultation Document

Information Security, Risk and Governance Framework and Policies

Document Control	
Title/Version	End of Consultation Document
Owner	Corporate Information Governance Group
Date Approved	2 December 2016

Description	Version		Considered by
First Draft	1.0	23 Nov 16	David Randall/ Hannah Lynch
Second Draft	2.0	25 Nov 16	David Randall/ Hannah Lynch
Final Draft	3.0	02 Dec 16	CIGG

Contents

Contents 2
1. Introduction 2
2. Feedback summary 2
3. Responses 2
4. Changes to original proposal 2
5. Timeline and Next Steps 7

Introduction

Consultation on the Information Security and Governance Framework and an associated suite of Information Governance Policies for Canterbury City Council, Dover District Council (including East Kent HR and East Kent Audit Partnership), Thanet District Council (including East Kent Services) and East Kent Housing commenced on 13 October 2016 and ended on 27 November 2016.

Thank you for all of the feedback during this period, it has been extremely productive and has informed the final proposals as outlined in this document and its appendices. This document should be read in conjunction with the original consultation paper.

Subject to the necessary approval at each Authority or body, the final policies will be published on the intranet site and will take effect from 1 January 2017.

Feedback summary

Feedback and comments from both the Trade Unions and staff were collected via the intranet pages and have been considered by the Corporate Information Governance Group (CIGG), which includes the SIRO and Deputy SIRO from each authority and representatives from EKS (ICT), EKHR, EKH and EKAP. These have informed the final framework and policies as outlined in this document. Some of the key themes have been collated and are included at section 4 of this document.

Responses

Feedback and comments were collated.

Changes to original proposal

The majority of the feedback received sought clarification around the application of the policies and procedures and/or suggested changes to the wording which do not significantly impact the structure or content of the policy or procedure. A summary of these are detailed below:

Policy	Feedback	Final action
Information Security, Risk and Governance Framework	None received	Adopt as drafted
Physical and Environmental Security	None received	Adopt as drafted
Password Policy	I'd place the comment about writing down/sharing passwords in the "Key message" section given how important it is. iOS allows a longer PIN that 4 characters although our current MDM policy prevents me from doing so. May be worth a caveat or clarification as, although the OS allows it, the device config does not. Typo: "Car Registration plates plates" - an extra "plates" should be removed.	Added to key message section of the policy. This is already stated within key messages in the policy so no further change required. Amended accordingly.

	Passwords not containing names - I'd argue over zealous. By the time the password is 12 characters long, the fact that 4 of those characters is my friend's name is irrelevant. I wouldn't permit a password like "Will Russell Tim 3" as it's people in the team I'm from but "Russell Parrot Building 4" would be fine (and once hashed not a problem as guessing "Russell" wouldn't give you the rest). App development standards: "Shall not store passwords in clear text or in any easily reversible form". Unfortunately this isn't achievable in a number of situations. Case in point: web application which requires a database password to be provided in a text based configuration file. A caveat to this clause along the lines of "wherever possible, shall not store passwords in clear text or in any easily reversible form" would allow both situations.	Edited the bullet point within the policy to reflect the comment. Suggested words inserted into the policy.
Internet Use Policy	None received	Adopt as drafted
E-Mail Acceptable Use Policy	Regarding the recent incident involving a member of staff clicking a link in an email. Some firms use a series of test emails sent to staff which contain links that used to monitor where additional training is required, for example the company sends a mail to staff advising a secure token is available for collection from the mailroom - the user clicks the link which flags on a report to identify which users require additional email security training. This pro-active approach can help to prevent situations where staff are negligent and also helps to ensure that all emails are treated with the same sense of cautiousness. Nothing to comment regarding emailing large attachments, can the policy clarify whether use of Dropbox/ we transfer and other such sites is okay?	References to internet policy corrected so that they now refer to the email policy. Additional wording added to bullet point to reflect this type of incident, however, not reflected the potential use of this tool in the policy itself. This has been discussed previously at the CIGG and would be a matter for the group. Added reference to secure file sharing solutions in the policy.
Wi Fi Policy	An issue here is that staff are not trained to spot a good Wi-Fi network from a malicious one. Should this come to a disciplinary I'd be querying what training the end user had to know if a network was good or bad. Additionally, they only have to	Wording amended in responsibilities section of the policy to reflect the feedback. Removed the requirement to 'satisfy' and replaced with a duty of care.

	satisfy themselves according to this policy ("you must satisfy yourself that the connection is trustworthy"). By that token, this is unenforceable as the end-user can claim they satisfied themselves and the employer would be unable to prove the employee was being neglectful. It may be better for this to be guidance/training than a policy which could be used in a disciplinary. Not sure how practical it is to require that 'you must satisfy yourself that the connection is trustworthy, before you connect to it.' In practice many public areas now offer 'free Wi-Fi', how are individuals supposed to differentiate between what is trustworthy and what is not?	
Removal Media Policy	Under "key messages" it gives the impression only "returning or visiting devices" must be AV scanned. This means I can plug my personal device in for the first time and use it without scanning the device. Perhaps simply change this to "any time a removable media device is to be connected to Organisation owned equipment it must be scanned by ICT"? The potential impacts of removable media incidents are very serious.	Edited the bullet point within the policy to reflect the comment. However, this was rejected by the CIGG as it was considered to be too draconian a control measure and would adversely impact on day to day operations. Therefore the original wording was retained. Practical procedures to be developed to balance the need for removable media risks to be mitigated, whilst allowing the business to operate effectively.
Remote Working Policy	None received	Adopt as drafted
Information Management Policy	None received	Adopt as drafted
Incident Management Policy	None received	Adopt as drafted
Payment Card Industry Data Security Standards Policy	None received	Adopt as drafted
Business Continuity Policy	None received	Adopt as drafted
Information Risk Management	None received	Adopt as drafted

Policy		
Information Sharing Policy	None received	Adopt as drafted
PSN Acceptable Usage Policy and Personal Commitment Statement	None received	Adopt as drafted
Digital Security Policy – Network Access and Availability	None received	Adopt as drafted
Digital Security – Monitoring and Standards	"All owned and managed devices must meet these criteria" - implies the same is true for servers and workstation (non-portable) computers. "The device must have the capability to detect, isolate and respond to malicious software" a switch can't. Perhaps a caveat of "capable devices must..."? Similarly on the next point. "Session Activity by User and Workstation" - paragraph is missing its ending. Might be worth not naming software we use, as if that has to change the policy has to be updated.	Edited the bullet point within the policy to reflect the comments. Edited the bullet point within the policy to reflect both comments.
Data protection Policy	I am writing in connection with the Data Protection Policy, in particular the requirement to destroy or dispose of the data when it is no longer required. I am aware that many older IT systems were not designed to be able to identify items of personal data or to delete them readily, if at all. How do we secure compliance with the Act when we cannot identify or delete data that is no longer required?	This is being addressed through the Data Protection Sub Group.

Timeline and Next Steps

Description of Activity / Action	**Date**
Formal adoption of policies and procedures by the CIGG	2 December 2016
Consideration by Cabinet for approval and adoption	9 January 2016
Framework and Policies to go live (retrospectively)	1 January 2017

Subject:	**GUIDANCE ON SUSPECT DEVICES, PACKAGES AND CALLS**
Meeting and Date:	**Cabinet – 9 January 2017**
Report of:	**David Randall, Director of Governance**
Portfolio Holder:	**Councillor Mike Conolly, Portfolio Holder for Corporate Resources and Performance**
Decision Type:	**Non-Key Decision**
Classification:	**Unrestricted**
Purpose of the report:	To adopt guidance as a Health and Safety policy for this Council.
Recommendation:	That the Guidance on Suspect Devices, Packages and Calls is adopted as a Health and Safety policy of the Council.

1. Summary

1.1 Local Authorities should remain alert to terrorist or other type attacks. Dover District Council has a responsibility to manage and minimise any risk by putting sensible and proportionate measures in place.

1.2 This guidance identifies the preventative measures and actions to follow in the unlikely event of any threat being received.

1.3 Cabinet is asked to approve the guidance as a Health and Safety policy.

2. Background

2.1 There is no intelligence or history to suggest Local Authorities are more likely to be subjected to a terrorist attack. Nonetheless Local Authorities should remain alert as being in the public sector brings increased risk through regular direct contact with members of the public. Dover District Council has a responsibility to manage and minimise any risk.

2.2 This guidance will enable this Council to implement preventative measures to minimise the risk of a threat and active measures to follow in the unlikely event of any device, package or call being received. The guidance aims to ensure that there is an understanding of the different types of threat, sensible and proportionate preventative measures are in place, such as an adequate level of security being in place and active procedures are in place to respond to a direct action.

2.3 If this guidance is adopted, suitable training will be provided to reinforce the messages. In addition, all members of staff have individual responsibility to support any security measures that are in place and in particular to remain vigilant.

3. Options for Consideration

3.1 Option 1. To adopt the guidance for this Council. This is the preferred option.

3.2 Option 2. To not adopt and rely on the vigilance of staff and ad hoc arrangements.

4. **Preferred Option**

4.1 Approve Option 1, which provides us with up to date guidance as a Health and Safety policy.

5. **Resource Implications**

5.1 There are no new resource requirements.

6. **Corporate Implications**

6.1 Comment from the Section 151: Finance has been consulted and has no further comment to add (VB).

6.2 Comment from the Solicitor to the Council: The Solicitor to the Council has been consulted in the preparation of this report and has no further comments to make.

6.3 Comment from the Equalities Officer: The report does not specifically highlight any equality implications, however in discharging their responsibilities members are required to comply with the public sector duty as set out in section 149 of the Equality Act 2010 http://www.legislation.gov.uk/ukpga/2010/15

6.4 Other Officers (as appropriate):

7. **Appendices**

Appendix 1 – Guidance on Suspect Devices, Packages and Calls

8. **Background Papers**

None

Contact Officer: David Randall, Director of Governance

Appendix 1

Guidance on Suspect Devices, Packages and Calls

SAFETY GUIDANCE NOTE No. 14
January 2017

1. Introduction

There is no intelligence or history to suggest Local Authorities are likely to be subjected to a terrorist attack. Nonetheless Local Authorities should remain alert as being in the public sector brings regular direct contact with members of the public. Dover District Council has a responsibility to manage and minimise any risk.

The Council will implement measures to follow in the unlikely event of any threat being received. They will ensure that there is an adequate level of security in place and suitable training provided. All members of staff have individual responsibility to support these security measures and in particular to remain vigilant.

2. Preventative measures to reduce the Risk from Attack

Dover District Council will take any action necessary to reduce the potential risks of any attack, as far as practicable. This will include:

- Improved security, including an expectation that all staff will challenge anyone in a secure part of the building who is not wearing a security pass.
- Assessing the risk in the light of current national and international climate or current terrorist campaigns.
- Assessing information from local police.
- Restricting access to a building or part of a building.
- Where appropriate train staff on the preventative measures.
- Provide aa weekly update to Customer Services of the Council's Incident Liaison Officer, Activation Officer and Duty Director

3. Preventative measures for dealing with Suspicious Packages & Postal Deliveries

Dover District Council will take all necessary steps following a risk alert to deter and detect anyone from delivering a suspicious package. This will include:-

- Assessing information from local police and postal services.
- Ensuring all external doors meet minimum requirements in respect of general standard and security.
- Lighting to be of a reasonable standard.
- Good housekeeping inside and outside the building.
- Appropriate awareness training for staff.
- Encouraging staff to remain vigilant at all times.
- Provide a weekly update to Customer Services of the Council's Incident Liaison Officer, Activation Officer and Duty Director.

4. Dealing with a Telephone/ Social Media Threat

Terrorists have in the past given telephone warnings of bomb explosions.

Staff may receive a warning that Council premises are at risk. Alternatively terrorist organisations may issue warnings to local authorities about other organisations where an explosion has been planned. In all cases it is important to escalate to your supervisor or manager who will liaise with the Duty Director and decide whether to contact the police immediately with full details of the call/ message. Because most telephone lines can be telephoned direct all staff have to be alerted to the possibility of receiving a bomb threat and how to deal with the call/ message.

The five key rules are:-

- Remain calm
- Try to obtain as much information as possible from the call/ message (see Annex B)
- Keep the line open even after the caller has hung up
- Report the call/ message to your supervisor or manager
- Your supervisor or manager must report the call/ message to the Activation Officer/Corporate Support Officer who will liaise with the Duty Director and decide whether to escalate to the police and whether and how to evacuate the building.

Action to be taken in the event of receiving a bomb threat is shown in Annex A and B. This information will be available to all staff.

5. Dealing with Suspicious Packages & Postal Deliveries

5.1 Recognising a Suspicious Package or Post

Postal Improvised Explosive Devices take many forms. They may come in any shape or size, parcels, envelopes or padded “jiffy bags”. They may explode or ignite when opened and sometimes before they are opened. They are usually designed to kill or maim the person who is opening them. Unless staff are aware of and looking for the tell-tale signs they may not notice anything amiss. Instead of being posted such devices may be delivered by hand or arrive via a courier.

Any of the following signs should alert members of staff to the possibility that a letter or package contains an explosive device:-

- Grease marks on the envelope or wrapping.
- An unusual odour such as marzipan or machine oil.
- Visible wiring or tin foil, especially if the envelope or package is damaged.
- The envelope or package may feel very heavy for its size.
- The weight distribution may be uneven; the contents may be rigid in a flexible envelope.
- It may have been delivered by hand from an unknown source or posted from an unusual place.
- If a package it may have excessive wrapping.
- There may be poor handwriting, spelling or typing.
- It may be wrongly addressed or come from an unexpected source.
- There may be too many stamps for the weight of the package.

All staff who might be required to open mail in the course of their work should be warned that, should they have any suspicions that a package may contain an explosive device, they should follow the five key rules:

- Remain calm.
- Put the package down gently and walk away from it.
- Don’t place the package into anything (including water) or place anything on top of it.
- If possible leave a distinctive marker near (not touching) the device.
- Report the suspect package immediately to your supervisor or manager.
- Your supervisor or manager must report to the Activation Officer/Corporate Support Officer who will liaise with the Duty Director and decide whether to escalate to the police and whether and how to evacuate the building.

6. Search Policy

Search teams will be formed from the Emergency Services that will search areas with advice from the Property Services Team. Council staff must not undertake searches of the building.

A telephone “cascade” system can be used with a main co-ordinator ringing several numbers and those people in turn ringing several others until all the teams have been alerted.

If a suspicious object is found, follow the golden rules at Annex A.

Annex A

ACTIONS TO BE TAKEN ON RECEIPT OF A BOMB THREAT

1 Remain calm and talk to the caller
2 Note the caller's number if displayed on your phone
3 If the threat has been sent via email or social media, see Annex B below
4 If you are able, record the call
5 Write down the exact wording of the threat

When Where What How Who Why Time

ASK THESE QUESTIONS & RECORD ANSWERS AS ACCURATELY AS POSSIBLE:

Where exactly is the bomb right now?	
When is it going to explode?	
What does it look like?	
What does the bomb contain?	
How will it be detonated	
Did you place the bomb? If not you, who did?	
What is your name?	
What is your address?	
What is your telephone number?	
Do you represent a group or are	

you acting alone?	
Why have you place the bomb?	
Record time call completed:	

INFORM YOUR MANAGER OR SUPERVISOR IMMEDIATELY

Name and telephone number of person informed:	

INFORM THE ACTIVATION OFFICER/CORPORATE SUPPORT OFFICER WHO WILL IMMEDIATELY LIAISE WITH THE DUTY DIRCTOR AND DECIDE WHETHER TO DIAL 999 AND INFORM THE POLICE

Time informed:	

This part should be completed once the caller has hung up and police/activation officer have all been informed.

Date and time of call:	
Duration of call:	
The telephone number that received the call:	

About the caller:	**Male**	**Female**	**Nationality**	**Age**
	☐	☐		

Threat language:	**Well-spoken**	**Irrational**	**Taped**	**Foul**	**Incoherent**
	☐	☐	☐	☐	☐

Caller's Voice:	**Calm**	**Crying**	**Clearing**	**Angry**	**Nasal**

			Throat			
Slurred	Excited	Stutter	Disguised	Slow	Lisp	*Accent
Rapid	Deep	Familiar	Laughter	Hoarse	Other (*please specify)*	

***What accent?**	
If the voice sounded familiar, who did it sound like?	

Background Sounds:

Street Noises	House Noises	Animal Noises	Crockery	Motor	
Clear	Voice	Static	PA System	Booth	Music

Factory Machinery	Office Machinery	Other (*please specify)*

REMARKS:

ADDITIONAL NOTES:

Signature:

Print Name:	
Date:	

Annex B

ACTIONS TO BE TAKEN ON RECEIPT OF A BOMB THREAT SENT VIA EMAIL OR SOCIAL MEDIA:

1. DO NOT reply to, forward or delete the message
2. If sent via email, note the address
3. If sent via social media, what application has been used and what is the username/ID?
4. Report the call/ message to your supervisor or manager.
5. Your supervisor or manager must report the call/ message to the Activation Officer/Corporate Support Officer who will liaise with the Duty Director and decide whether to escalate to the police and whether and how to evacuate the building.
6. Preserve all web log files for your organisation to help the police investigation (as a guide, 7 days prior to the threat message and 48 hours after).

IMMEDIATELY HAND A COPY OF THIS FORM TO THE ACTIVATION OFFICER/CORPORATE SUPPORT OFFICER

DOVER DISTRICT COUNCIL

NON-KEY DECISION **EXECUTIVE**

CABINET – 9 JANUARY 2017

EXCLUSION OF THE PRESS AND PUBLIC

Recommendation

That, in accordance with the provisions of the Local Authorities (Executive Arrangements) (Access to Information) (England) Regulations 2000, the public be excluded from the remainder of the meeting for the following items of business on the grounds that they involve the likely disclosure of exempt information as defined in the paragraph of Schedule 12A of the 1972 Act set out below:

Item Report	Paragraph Exempt	Reason
Compensation Payment	3	Information relating to the financial or business affairs of any particular person (including the authority holding that information)

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted