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

Corporate Information Governance Group (CIGG)

Information Governance Policy Framework

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.