DOVER DISTRICT COUNCIL

Democratic Services
White Cliffs Business Park
Dover
Kent CT16 3PJ

Telephone: **(01304) 821199**
Fax: **(01304) 872453**
DX: **6312**
Minicom: **(01304) 820115**
Website: **www.dover.gov.uk**
e-mail: **democraticservices@dover.gov.uk**

10 May 2023

Dear Councillor

NOTICE OF DELEGATED DECISION – (DD58 22) DATA PROTECTION POLICY 2023

Please find attached details of a decision taken by Mrs Louise May, Strategic Director (Corporate and Regulatory), to update the Council's Data Protection Policy.

As a non-Key Officer Decision, call-in does not apply (paragraph 18(a) of Part 4 (Rules of Procedure) of the Constitution).

Members of the public who require further information are asked to contact Democratic Services on 01304 872303 or by e-mail at democraticservices@dover.gov.uk.

Yours sincerely

Democratic Services Officer

ENCL

1 **NOTICE OF DELEGATED DECISION - (DD58 22) DATA PROTECTION POLICY 2023** (Pages 2-25)

Decision Notice

Delegated Decision

Decision No:	**DD58**
Subject:	**DATA PROTECTION POLICY 2023**
Date of Decision:	**4 April 2023**
Notification Date:	**10 May 2023**
Implementation Date:	**9 May 2023**
Decision taken by:	**Louise May, Strategic Director (Corporate and Regulatory)**
Delegated Authority:	**Delegation C58 to the Strategic Director (Corporate and Regulatory) of Section 6 (Scheme of Officer Delegations) of Part 3 (Responsibility for Functions) of the Constitution as follows: 'To exercise the powers and functions of the Council in relation to the GDPR and the Data Protection Act 2018.'**
Decision Type:	**Executive Non-Key Decision**
Call-In to Apply?	**No (*Call-in does not apply to non-Key Officer decisions*)**
Classification:	**Unrestricted**
Reason for the Decision:	To ensure compliance with the Council's obligations under the Data Protection Act 2018 and the UK GDPR.
Decision:	To approve the revised Data Protection Policy.

1. **Introduction**

1.1 The Council has a statutory duty to meets its obligations as set out within Data Protection Legislation. Information held by the Council is a valuable asset and we must ensure that it is protected from accidental or deliberate damage, disclosure or unauthorised modification or destruction.

1.2 The Council's East Kent Corporate Information Governance Group annually reviews the corporate information governance policies. The data protection policy requires more frequent reviews to ensure that it is up to date with legislation, guidance issued by the Information Commissioner's Office, and changes to our own practices and procedures for the processing and sharing of personal information.

1.3 The Data Protection Policy has been revised and updated by the Council's Data Protection Officer, Governance Officer and Senior Information Risk Owner. Minor changes have been made throughout each section to reflect the way in which the Council processes data. More significant changes include additions to information sharing and the Kent and Medway Information Sharing Agreement, and updates to the roles and responsibilities section as the role of the Senior Information Risk Owner (SIRO) is now held at director level.

2. **Any Conflicts of Interest Declared?**

None.

3. **Supporting Information**

See attached Data Protection Policy 2023.

Data Protection Policy

Contents

1.0 Introduction

1.1 Dover District Council ("the Council") has a statutory duty to meets its obligations as set out within Data Protection Legislation. Information held by the Council is a valuable asset and we owe a duty, both to the members of the public and to those who work for the Council, to protect their personal data from accidental or deliberate damage, disclosure or unauthorised modification or destruction.

1.2 This document sets out the Council's policy on data protection affirming the enhanced individual rights and the responsibilities of those who work with personal data as required by current data protection legislation.

1.3 This policy applies to all personal data processed by the Council regardless of format, and any individual processing personal data held by the Council.

1.4 The Council states that, in general:

- it does not seek to offer goods or services to data subjects in the European Union, and
- it does not seek to monitor behaviour which occurs within the European Union

Therefore the General Data Protection Regulation 2016 does not apply to the Council.

Processing of personal data the Council undertakes is under UK Data Protection Legislation including; the Data Protection Act 2018, UK General Data Protection Regulation (UK GDPR) and the Privacy and Electronic Communication Regulation 2003.

2.0 Relationship with other policies and procedures

2.1 This policy is underpinned and supplemented by other policies and procedures within the Council, they include: -

- Retention Schedules;
- Subject Access Request Procedure;
- Personal Data Breach Procedure;
- Data Protection Impact Assessment Procedure and Form (DPIA);
- Physical & Environmental Security Policy
- Information Management Policy
- Acceptable Use Policy
- Digital Security Policy
- The Council's Privacy Statement and Corporate Privacy Notice, along with specific Departmental Privacy Notices; and
- Record of Processing Activities in the UK GDPR and will incorporate all Departmental Information Asset Registers
- CCTV and Body Worn Cameras

3.0 Policy

3.1 The Council aims to operate in a professional manner at all times and to be open and accountable for the data it processes.

3.2 The ICO is responsible for ensuring compliance with Data Protection legislation; and has extensive powers under the UK GDPR to take action against organisations which breach data protection law. This includes substantial fines as well as other regulatory action such as enforcement notices.

3.3 Any breaches of Data Protection legislation must be reported to the Data Protection Officer ("DPO") in accordance with the Council's breach reporting procedure.

3.4 The DPO has responsibility for monitoring compliance with Data Protection Legislation and will be the first point of contact for any cases of doubt.

3.5 This policy covers personal data, special categories of personal data and criminal offence data as defined by data protection legislation.

3.6 The Council will process data in accordance with the following 6 principles and the other requirements of UK GDPR, which are summarised as follows:

- Personal information will be obtained and processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency');
- It will be obtained and processed for specified purposes ('purpose limitation') and not processed for any incompatible purposes;
- Personal information shall be adequate, relevant and not excessive in relation to the purpose for which it is processed ('data minimisation');
- Personal information shall be accurate and kept up to date where necessary; having regard to the purposes for which they are processed, ensuring they are erased or rectified without delay ('accuracy');
- Personal information will not be kept for longer than is necessary for the purpose for which it is processed except where the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation'); and
- Appropriate technical and organisational measures shall be taken to ensure the personal information is secured against unauthorised/unlawful processing, accidental loss, damage or destruction ('integrity and confidentiality').

3.7 The UK GDPR also introduces an accountability principle. This is an overarching requirement to objectively demonstrate compliance with all the above principles in the UK GDPR.

4.0 Legal Definitions

4.1 The following definitions shall apply:

a) Data Protection Legislation means:

- The UK General Data Protection Regulation ("UK GDPR"),
- Data Protection Act 2018 (“DPA”)
- Law Enforcement Directive;
- The Privacy and Electronic Communications (EC Directive) Regulations 2003; and
- Any other applicable law concerning the processing of personal data and privacy.

b) Personal Data means any information, which either directly or indirectly, relates to an identified or identifiable natural living person. Identifiers include name, address, and date of birth, postcodes, unique identification numbers, location data, online identifiers (such as an IP address), pseudonymised data and information relating to a person's social or economic status.

c) Special Category Data means personal data consisting of information as to:

- The racial or ethnic origin of the data subject;
- Political opinions;
- In some cases an individuals gender;
- Religious beliefs or other beliefs of a similar nature;
- Trade union membership;
- Physical or mental health or condition;
- Biometric and/or genetic data;
- Sex life or Sexual Orientation;

d) Criminal Offence Data means personal data consisting of information as to:

- The commission or alleged commission by the data subject of any offence; or
- Any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

e) Processing in relation to Personal Data, means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

f) Data Subject means an individual who is the subject of personal data.

g) Controller means a person or organisation who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which, any personal data is, or is to be, processed. A data controller may also act jointly with another organisation to process personal data.

h) Processor, in relation to personal data, means any person or organisation (other than an employee of the data controller) that processes the data on behalf of the controller.

5.0 Roles and Responsibilities

5.1 The Council is responsible for ensuring that personal data is processed in accordance with Data Protection Legislation. These responsibilities include but are not limited to ensuring that personal data is kept securely, in the right hands and that it is accurate. However, there are specific responsibilities allocated to certain individuals.

a) The Council shall ensure that:

- It pays its fees to the Information Commissioner's Office;
- It has specialist staff with specific responsibility for ensuring compliance with Data Protection Legislation;
- Staff processing personal data understand that they are responsible for complying with the Data Protection Legislation including ensuring that processing activities meet a lawful basis for processing and that processes are documented;
- Staff processing personal data are appropriately trained to do so and continue to be provided with annual data protection and cyber security training;
- All staff are provided with appropriate data protection support and guidance.

b) Data Protection Officer

The Solicitor to the Council is the Council's designated DPO responsible for supporting the council in meeting its obligations under data protection legislation.

The role, which is a statutory requirement, has responsibility for:

- Monitoring the Council's ongoing compliance;
- Providing advice and guidance on all data protection matters;
- Ensuring that mandatory data protection training is provided to all Council staff;
- Advising on the development of policies and procedures, DPIAs and conducting internal audits;
- Analysing all incidents, determining when a breach will be a breach, and reporting to regulatory authorities as applicable;
- Acts as the single point of contact for all data subjects;
- Act as the single point of contact for the Information Commissioner's Office and any other bodies engaged in the application of data protection legislation.

The Council will support the DPO by providing resources to undertake tasks and access to personal data and processes and operations and to maintain expert knowledge. The DPO must be able to perform their duties in an independent manner and the Council will not give the DPO instruction on exercising their role.

c) The Strategic Director (Corporate and Regulatory Services)

Is the Senior Information Risk Owner (SIRO) of information risk management and is responsible for leading and fostering a culture that values, protects and uses information in a

manner which benefits the Council and its service users. This role is held at Strategic Director level.

This role is responsible for:

- Together with the Data Protection Officer, providing Information Governance (IG) support and guidance to the Council to ensure that staff are aware or their responsibilities and obligations in relation to data protection and cyber security;
- Working across the Council's functions in the application of data protection and information security;
- Developing the Council's Information Governance policies and procedures;
- Reviewing, assessing, and monitoring corporate information risk.

d) Governance Officer

The Council's Governance Officer has day to day responsibilities for data protection working alongside and deputising for the Data Protection Officer to advise the Council, minimise information risk and ensuring compliance with Data Protection Legislation. They also support the Senior Information Risk Owner in their tasks.

This role has responsibility for:

- Together with the DPO/SIRO provide support and guidance to the Council to ensure that staff are aware or their responsibilities and obligations under data protection;
- Developing, implementing and maintaining the Council's information governance and data protection functions and responsibilities alongside the Data Protection Officer;
- Completing, reviewing, Identifying, monitoring, and advising on data protection risks in DPIAs;
- Ensuring privacy notices, retention schedules and information asset registers are being created, maintained and complied with;
- Reviewing of information governance policies;
- Personal data breaches; investigating, analysing risks, advising on mitigations, deciding on notification requirements;
- Providing Information governance and UK GDPR/DPA advice and guidance to all staff and departments of the Council;
- Ensuring the required legal documentation is in place when the Council uses a data processor to process personal data on the Council's behalf. This includes data processing agreements and schedules of processing activities for contracts, and data sharing agreements for controller-to-controller sharing.

e) Information Asset Owner (IAO)

This is an individual who is responsible for ensuring that specific information assets are handled and managed appropriately. IAO's are decision makers across information they own in their relevant service area.

This role has responsibility to:

- Act as a source of advice and expertise to in their service;

- Ensure compliance with the provisions of data protection legislation in respect of the IAO's personal information assets, in accordance with the Council's policies;
- Work effectively with the DPO/SIRO & Governance Officer;
- Ensure that registers of personal data held are compiled and maintained;
- Provide updates to the SIRO about the security and use of the asset.

f) Council Staff and Councillors

All staff and Councillors shall ensure they process information in accordance with Data Protection legislation. This includes complying with related policy requirements and undertaking mandatory annual data protection and information security training.

6.0 Record of Processing Activity

6.1 The Council shall create maintain a written record of its data processing activities.

6.2 The Information Governance team and each department shall be responsible for creating and maintaining the record of processing activity in accordance with UK GDPR Article 30.

7.0 Privacy Notices

7.1 The Council shall ensure that privacy notices are published on the council website. This shall:

- Explain the purposes for which the Council will process the data collected;
- Detail the lawful basis and legal gateway for personal data processing and sharing;
- Detail the existence of the Rights available to data subjects to exercise (UK GDPR A12-22)
- Make data subjects aware that they have the right to lodge a complaint with a supervisory authority;
- Explain where the Council will keep information and why we hold it and for how long;
- Explain where the Council gets personal data from and whom it shares personal data with;
- Provide contact details of the DPO to allow requests for further information;

7.2 In certain circumstances, it will be necessary for service areas to provide additional information, to that described within their own privacy notice, for example when and where the Council might share personal data with others.

7.3 A copy of the privacy notice shall be provided on request and free of charge. This is also available on the Council's Website.

7.4 The Council provides the necessary privacy information to data subjects through:

- The Council's Corporate Privacy Notice;
- Service specific privacy notices;
- Just in time notices.

8.0 Data Protection Impact Assessment (DPIA)

8.1 The Council shall use a DPIA from the early stages of any project where certain types of high risk processing are present e.g. large scale processing, systematic monitoring or processing special category data. The DPIA shall be used to identify and reduce privacy risks of a project. A DPIA will enable us to systematically and thoroughly analyse how a particular project, processing activity or system will affect the privacy of the individuals involved, while allowing the aims of the project to be met whenever possible.

8.2 Staff shall consult with the Information Governance team at an early stage to identify DPIA requirements. The Information Governance team will provide adequate advice and assistance for conducting a DPIA.

8.3 The DPO shall be consulted on all DPIAs.

9.0 Data Security

9.1 The Council shall ensure it has an information security management system in place which aims to reduce the risk of theft, loss or unlawful processing of personal data.

- Security policies and procedures shall be made available to all staff;
- The Council shall take all reasonable steps to adequately train all staff;
- The Council shall record and investigate all personal data breaches, led by the DPO;
- Where it is determined that a breach results in a high risk to the rights and freedoms of an individual(s) the Council shall report the breach to the Information Commissioner's Office within 72 hours of becoming aware;
- Where it is determined that a breach results in a high risk to the rights and freedoms of an individual(s) the council shall inform the individual(s) without undue delay.

10.0 Reporting a Personal Data Breach

10.1 Data Protection Legislation requires the Council to notify personal data breaches to the ICO and, in certain instances, the data subject. This will be done by the DPO; staff and councillors should not attempt to notify the data subject or the ICO.

10.2 The Council has procedures for dealing with any suspected personal data breaches and will notify data subjects or the ICO where legally required to do so, and when necessary to protect the rights and freedoms of the of the data subject(s).

10.3 If staff or councillors know or suspect that a personal data breach has occurred, they must immediately notify the DPO by reporting it as a data or cyber security breach at:

Report a Personal Data or Cyber Security Breach

10.4 Once the breach reporting form is completed it will be sent to the DPO, SIRO and Governance Officer. They will be in contact to review the data breach and advise on mitigation to any risk that may be caused to the data subject(s) or the Council.

11.0 Payment Card Industry Data Security Standard PCI (DSS)

11.1 The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that companies processing, storing or transmitting credit or debit card information maintain a secure environment.

11.2 The Council is required to maintain these standards and will comply with this requirement as part of its normal data security practices.

12.0 Transfers to Third Parties

12.1 If the Council is asked to transfer personal data to any third parties such as other public authorities e.g. the police, Department for Works & Pensions, HMRC; or contractors, consultants, external Legal Advisers, such transfers will only be completed in accordance with Data Protection Legislation.

12.2 Approval in high risk circumstances will be required by the DPO.

12.3 The Council will take reasonable steps to ascertain the identity of any third party and generally seek requests in writing.

12.4 Information over the phone will only be given when the member of staff or councillor concerned is confident they knows to whom they are speaking, and that disclosure is appropriate.

12.5 The Council will release information where it is obvious that consent has been obtained.

12.6 The Council will exercise particular care in relation to disclosure of special categories of personal data and criminal offence data and will only disclose to third parties in limited circumstances. Normally the Council will only do this where it is necessary for the exercise of their statutory obligations. Or where the disclosure is being made in order to investigate crime and non-disclosure would prejudice the investigation, e.g. to the police.

13.0 International Transfers

13.1 The Council shall not transfer personal data to a third countries or international organisations unless there is a legal requirement to do so or it can be evidenced that appropriate safeguards are in place as required by Data Protection Legislation.

13.2 Any data sharing of personal data outside of the UK should only be undertaken in accordance with ICO guidelines with approval from the DPO.

13.3 Where it is identified that an international transfer of personal data is necessary, the Council may seek appropriate legal advice.

14.0 Contracts

14.1 Contracts shall include measures to ensure personal data is handled in accordance with Data Protection Legislation, in particular:

- Personal data shall only be supplied for the agreed purposes as set out in the contract and shall not be processed for any other reason;
- The Council shall ensure that before personal data is shared with a third party as part of a contract, and that appropriate security controls are in place.
- When there is a controller and processor relationship, a data processing agreement shall be in place pursuant to UK GDPR A28 detailing the personal data processing instructions determined by the Council.

15.0 Information Sharing

15.1 The Council will take the following steps when sharing information with third parties:

- The Council shall ensure that information is shared only when it is permitted by Data Protection Legislation.
- The Council shall ensure that when information is shared it is justified and a lawful basis has been identified as set out in Data Protection Legislation.
- The Council shall ensure that adequate security is in place to protect the data when it is shared with another organisation and that information sharing arrangements are documented in a transparent manner.
- The Council shall ensure the secure transfer of personal data between itself and other organisations.
- The Council shall ensure that information sharing agreements exist between itself and partnership agencies, organisations may have signed up to the Kent & Medway Information Sharing Agreement.
- The Information Governance team shall provide the council with guidance on information sharing in the context of systematic sharing and sharing in ad-hoc, one off circumstances.

15.2 Information Sharing may be conducted under the Kent & Medway Information Sharing Agreement (K&MISA)

- The K&MISA is a high-level agreement between Kent local authorities and a number of public organisations in Kent and Medway. Its aim is to facilitate more effective data sharing across Kent and Medway.
- Canterbury, Dover and Thanet are each signatories to the agreement which will form the basis of our policy when sharing data with other signatories to the agreement.

15.3 When conducting information sharing under the K&MISA Councils must have identified a legal gateway and completed either the one off or repeat data sharing document detailing the specifics of information sharing. This will include:

- Who you are sharing with;
- What you will be sharing (personal/special category/criminal offence data);
- Your purpose for sharing;
- Your legal gateway to enable the lawful sharing of information;
- Duration and frequency of sharing.

16.0 Individual Rights

16.1 Data Protection Legislation provides the following rights:

- The right to be informed. Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR. The Council must provide individuals with information including:
    - the purposes for processing their personal data,
    - the retention periods for that personal data, and
    - who it will be shared with. We call this 'privacy information;
- The right of access. Individuals have the right to access their personal data;
- The right to rectification. The UK GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete;
- The right to erasure. The UK GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'. This is not an absolute right and only applies in certain circumstances;
- The right to restrict processing. Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances;
- The right to data portability. The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. This is not an absolute right and only applies in certain circumstances;
- The right to object. The UK GDPR gives individuals the right to object to the processing of their personal data in certain circumstances;
- Rights in relation to automated decision making and profiling. In particular, the right to be told of the existence of automated decision-making, including profiling and in those cases at least, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
- The right to lodge a complaint with the ICO.

17.0 Lawfulness, Fairness, Transparency

17.1 Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

17.2 The Council may only collect, process and share personal data lawfully, fairly and transparently and for specified purposes. Data Protection Legislation only allows the Council to process personal data for specified lawful purposes. These restrictions are not intended to prevent processing but ensure that the Council processes personal data fairly and in accordance with the rights of the data subject.

17.3 The UK GDPR allows processing for specific purposes, some of which are set out below:

(a) the data subject has given their consent;
(b) the processing is necessary for the performance of a contract;
(c) to meet our legal obligations;
(d) to protect the data subject's vital interests;
(e) required for the performance of a public task on grounds of necessity, this takes two forms:

- because we are carrying out a specific task in the public interest (e.g. providing homelessness services), where the task is laid down by the law (i.e. the overall task is contained in a statute, regulation, statutory guidance or laid down by case law); or
- because we are exercising our own official authority (e.g. fulfilling our duties, carrying out our functions or exercising our powers), where that authority is laid down by the law (i.e. the overall authority is contained in a statute, regulation, statutory guidance or laid down by case law).

(f) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices.

In order to rely on the public task lawful basis, the processing must be strictly required for us to perform the relevant public task. This means that if a less privacy invasive course than sharing personal information is available then we should adopt the less invasive course. The Council must identify and document the legal ground being relied on for each processing activity.

17.4 The Council will only collect and process personal data for one or more of the lawful basis' set out in Article 6 of the UK GDPR. The Council will identify the lawful basis before processing personal data. This must be appropriately documented.

17.5 There are six available lawful basis for processing Personal Data:

- Consent: express consent must be freely given, informed and evidenced by a clear affirmative action. It must be given by an unambiguous statement or by clear affirmative action signifying the data subject's agreement to the processing. In practice this means that wherever possible consent should be obtained in writing and signed by the subject with clear wording in plain English explaining precisely what they are agreeing to. Where written consent is not possible, verbal consent can be given but the terms of the consent must be clearly given to the subject and a written record of the consent kept;
- Contract: necessary for the performance of a contract with the Data Subject (including specific steps before entering into a contract);
- Legal Obligation: necessary to comply with a legal obligation to which the Council is subject;
- Vital Interests: necessary to protect the life of the data subject or of another natural person;

- Public Task: necessary to perform a task in the public interest or for the Council's official functions, and the task or function has a clear basis in law.
- Legitimate Interests: necessary for the council's, or third parties, legitimate interests in circumstances where the Data Subject's right to privacy does not override those legitimate interests. Notably, this legal basis is unavailable for public authorities such as the Council when performing their public tasks.

17.6 Personal Data, especially special category personal data, about employees and members of the public is shared only with staff that need to know the information in order to carry out their task(s). This may involve sharing information between individuals in different departments, so long as they are for compatible purposes.

17.7 Where appropriate, the Council will set up protocols to clarify how this operates in practice to ensure that only those people who have a need to know are able to access personal data of a data subject.

17.8 The Council will only collect and process special category personal data if one of the conditions set out in Article 9 of the UK GDPR or Schedule 1 of the Data Protection Act 2018 have been satisfied. This is in addition to satisfying one of the conditions in Article 6 of the UK GDPR. We have set out each of the conditions under Article 9 of the UK GDPR that could potentially be relevant for Council's activities:

The Council will rely on one or more (subject to the purpose of the Council's activity) of these ten available lawful bases to for processing special category data as provided under Article 9 of the UK GDPR:

- Explicit Consent: freely given, informed and evidenced by a clear affirmative action;
- Employment, social security or social protection law: necessary to meet legal obligations in these specific areas
- Vital Interests: necessary to protect the life of the data subject or another individual where they are physically or legally incapable of giving consent;
- Not-for-profit Bodies: processing carried out by a political, philosophical, religious or trade union;
- Deliberately made public by the Data Subject: data that has manifestly been placed in the public domain by the Data Subject;
- Legal Claims: necessary for establishing, exercising or defending legal rights;
- Substantial Public Interest: necessary for reasons of substantial public interest e.g. official functions, statutory purposes, equal opportunities or preventing or detecting unlawful acts;
- Health and Social Care: necessary to preventative or occupational medicine, for the assessment of the working capacity of an employee, medical diagnosis, provision of health or social care or treatment or management of health and social care systems;
- Public interest in the area of Public Health: such as threats to health or ensuring high standards of healthcare; and
- Archiving Purposes: public interest, scientific and historical research purposes or statistical purposes.

17.9 Data Protection Legislation makes special provision for the processing of criminal allegations, convictions and offences, or related security measures . In circumstances

where the Council collects and process a Data Subject's criminal offences data, this is done under the lawful basis that the Council is exercising its legal obligation as a public authority ; and it is necessary for reasons of substantial public interest for the purpose of complying with the provisions of UK GDPR as supplemented by the Data Protection Act 2018 (DPA). This is in addition to first, a lawful basis for processing under Article 6 of the UK GDPR.

17.10 A copy of the Appropriate Policy document for processing Special Category Data and Criminal Offence Data is appended to this policy (Appendix 1).

18.0 Children

18.1 Generally, Children have the same rights as adults under UK GDPR. This includes right to object to the use of their information, right to erasure, right to modify and right to be informed. Children can exercise these rights as long as they are competent to do so. And where they are not considered to be competent, an adult with parental responsibility may usually exercise the child's data protection rights on their behalf.

18.2 The Council understands that children need particular protection when collecting and processing their personal data.

18.3 When relying on consent, the Council will ensure it makes reasonable efforts to verify that children give a valid consent. The Council will endeavour to ensure that the child understands what they are consenting to.

18.4 Wherever the Council is relying on consent and the child does not understand what they are consenting to, the Council will obtain consent from whoever holds parental responsibility for them whilst ensuring we take reasonable steps in ascertaining that the person giving consent does, in fact, hold parental responsibility for the child.

18.5 When relying on 'necessary for the performance of a contract' we consider the child's competence to understand what they are agreeing to, and to enter into a contract.

18.6 When the Council rely upon 'public interests' as the basis for processing, as well as to provide services that we are under a statutory obligation to provide, the Council will balance the public's interests in processing the personal data against the interest and fundamental rights and freedoms of the child.

18.7 Where a child's right to be informed is being exercised, the Council will provide the child with the same information about their personal information as it will provide to adults. This will be presented in a clear, concise and plain manner, including an explanation on the risks inherent in the processing and safeguards we have in place.

18.8 The Council will regularly review its safeguarding mechanisms for holding and processing children's personal information, particularly around verification when relying on consent for its processing. Notably, the Council will strive to rely on other lawful bases asides from consent for processing children's information where it can.

19.0 Right of Access to Personal Data

19.1 In addition to the rights under this policy, any person whose personal data is processed by the Council has a right to ask the Council, about the personal data which the Council holds.

19.2 Within one calendar month of a request and free of charge, a data subject is entitled to:

- Be told whether personal data, of which they are the subject, is held in the Council's records, or otherwise processed by the Council; and
- Given a description of the personal data, the purpose for which the data is being or may be processed and the persons or classes of persons to whom the data has been or may be disclosed; and
- Have communicated to them in an intelligible form the information constituting the personal data held about them and any available detail as to the source of that information; and
- Be told the envisaged period for which the data will be stored or, if not possible, how it will be decided when it will be destroyed; and
- Be informed of their right to erasure of personal data; the right to rectification of data; to restriction on processing; and the right to object to processing; and
- Be informed of their right to complain to the ICO.
- Know of the existence of any automated decision-making, including profiling, and in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

20.0 Access to Personal Data Refusal

20.1 Data Protection Legislation allows the Council to refuse an individual's request to access personal data if allowing access would adversely affect the rights and freedoms of other. Examples of where this may apply are as follows:

- It would identify another individual/organisation that has not consented to the disclosure.
- It is important to note that organisations are not covered by Data Protection legislation so information about them may be disclosed. However, to avoid any claims of breach of confidentiality, their consent should be sought and disclosure should only be made without their consent if it cannot reasonably be obtained and it is reasonable in all the circumstances to make disclosure;
- It is legally privileged correspondence;
- The information consists of a reference given or to be given in confidence by the employer for:
    - the education, training or employment of the worker
    - the appointment of the worker to any office
    - the provision by the worker of any service
- The information is held for:
    - the prevention of the detection of crime; and/or;
    - the apprehension or prosecution of offenders; and/or

- the assessment or collection of any tax or duty or any other imposition of a similar nature where access would be likely to prejudice any of the above matters;
- the information was provided in confidence by a third party;
- in the opinion of the Council or a health professional it would be likely to cause serious harm to the physical and/or mental health of a resident or another person.

This list is not exhaustive; refer to data protection legislation for other examples.

21.0 Objection to processing

21.1 Individuals have the right to object to processing by the Council for the performance of a task in the public interest and/or their exercise of official authority. The same rules apply if the Council is relying upon legitimate Interest as its lawful basis when not acting as a public authority. In these instances, where an individual object, the Council must stop processing the personal data unless:

- The Council can demonstrate compelling public interest or legal obligation for the processing, which override the interests, rights and freedoms of the individual; or
- The processing is for the establishment, exercise or defence of legal claims.

22.0 Withdrawal of consent

22.1 An individual has the right to withdraw consent at any time. It shall be as easy to withdraw as to give consent.

22.2 If the basis on which personal information is being processed is the consent of the individual, then that processing must stop.

22.3 It may be that another reason for processing can be relied on such as public interests and fulfilment of a legal obligation.

22.4 In practice a withdrawal of consent is likely to be accompanied by a request to erase in which case the Council will need to rely on one of the other exceptions to erasure e.g. overriding public interest or legal obligation.

23.0 CCTV

23.1 Images and audio recordings of identifiable individuals captured by Closed Circuit Television (CCTV) amount to personal data relating to that individual and will be subject to the same provisions and safeguards afforded by Data Protection Legislation as other types of recorded information.

23.2 Each CCTV system will have its own site or task specific objectives. These could include some or all of the following:

- Protecting areas and premises used by council officers and the public;
- Deterring and detecting crime and antisocial behaviour;

- Assisting in the identification of and apprehension of offenders;
- On-site traffic and car park management;
- Monitoring traffic movement;
- Identifying those who have contravened parking regulations;
- Assisting in traffic regulation enforcement;
- Protecting council property and assets;
- Assisting in grievances, formal complaints and investigations;
- Surveying buildings, land and highways for the purpose of maintenance and repair.

23.3 The Council will ensure that any use of CCTV is necessary and proportionate to achieve its objective and any introduction of CCTV for a new purpose will be subject to a Data Protection Impact Assessment prior to being used.

23.4 The council will ensure that clear notices are in place identifying when an individual is entering an area that is monitored by CCTV. The notice will identify the Council as the organisation responsible for the recording and will state the purpose for which the recording is taking place along with contact details for further information.

23.5 CCTV recordings shall be kept securely, and access will be restricted only to those staff that operate the systems or make decisions as to how the recordings will be used.

23.6 Data subjects are able to exercise their rights in respect of any personal data relating to them that has been captured in a CCTV recording. Such requests will be considered in accordance with the guidance on individual rights. Any request by a third party (a person or organisation who is not the data subject or an employee of the Council) will be considered in accordance with Data Protection Legislation.

24.0 Equality & Diversity

24.1 The Council aims to ensure that its implementation is proactively inclusive with reference to the nine protected characteristics: ethnicity, religion or belief, gender, sexual orientation, gender reassignment, disability, age, marriage and civil partnership or pregnancy and maternity.

25.0 Compliance with this Policy

25.1 The Council recognises that compliance with this policy is important. Breach of Data Protection Law can be a criminal offence. In particular, knowingly obtaining, accessing or disclosing personal data maliciously.

25.2 The Council will consider disciplinary proceedings for any staff that breach this policy.

26.0 Information Commissioner's Office

26.1 The Information Commissioner's Office (ICO) is the supervisory body for data protection in the UK. Notably, the ICO has greater enforcement and sanctions powers under the UK GDPR. This includes powers to:

- Issue fines for breaches
- Investigative powers – such as the ability to request information, carry out data protection audits and access physical premises;
- Supervisory authorities are also given other corrective powers besides fines, including the power to issue warnings and reprimands; and
- The power to order compliance and to suspend or limit processing or data flows.

26.2 The Council will comply fully with all requests from the Information Commissioner's Office to investigate and/or review the Council's data processing activities.

26.3 The Council will have regard to advice and guidance produced by the Information Commissioner's Office as far as it relates to the council's data processing activities.

26.4 The Council will take into account any code of practice published by the Information Commissioner's Office and will endeavour to align its own practices accordingly.

27.0 Councillors

27.1 There are three ways in which Councillors might use personal data:

- when considering issues and making decisions as part of the Council's business – for example in committees or working groups. In this circumstance the Council is the data controller.
- as a member of a political party canvassing for votes or working for a party. In this circumstance the political party is the data controller.
- undertaking casework. In this case the Councillor is the data controller.

27.2 Where a Councillor is representing a constituent who has made a complaint, the Councillor's lawful basis for processing the personal information is where it is needed for the performance of a task carried out in the public interest. Sensitive personal information is processed for reasons of substantial public interest and Schedule 1 Part 2 of the Data Protection Act 2018 'elected representatives responding to requests'. The Council will not generally seek to rely on consent as the lawful bases for processing in these circumstances.

27.3 In representing their constituents, councillors may share personal information with the Council, other Councillors and the Member of Parliament.

27.4 Personal information held by the Council should not be used by councillors for political purposes.

27.5 When campaigning for election as a member of a political party, candidates can use personal information, such as mailing lists, legitimately held by their parties. However, personal information councillors hold in their role as representatives of local residents, such as complaints casework, should not be used without the consent of the individual.

27.6 Councillors take appropriate security measures to protect their constituents' personal information. They must take into account the nature of the information and the potential harm to individuals. They should consider what technical and organisational measures, such as use of passwords, computer access privileges, procedures and training, are appropriate to keep information safe.

27.7 Councillors will keep personal information for the minimum period necessary, usually no longer than four years. All information will be held securely and disposed of confidentially.

28.0 Policy Review

28.1 This policy will be reviewed by the Council from time to time.

29.0 Policy Compliance

29.1 If you do not understand the implications of this policy or how it may apply to you, seek advice from the DPO.

Document Control

Document Control	
Title/Version	Data Protection Policy
Owner	Corporate Information Governance Group

Revision History			
Revision Date	**Reviewer(s)**	**Version**	**Description of Revision**
14/06/2018	CIGG	1.0	
11/07/2019	Joe Couchman & Harvey Rudd	2.0	
08/11/2019	Policy Suite Subgroup	2.1	
01/05/2020		2.2	
14/09/2021		3.0	
15/03/2022	Policy Suite Subgroup	3.1	
08/02/2023	Data Protection Officer/Governance Officer & Senior Information Risk Owner	3.2	

Appendix 1 Appropriate Policy Document

Processing Special Category Data and Criminal Records Data

1. This is an appropriate policy document that sets out the Council's procedures when processing special category and criminal records personal data.

2. Special category data and criminal records data are both forms of personal data that warrant additional levels of care due to its sensitivity, this policy provides assurance of that care and the requirements under data protection legislation.

3. The Data Protection Act 2018 sets out the requirements for an appropriate policy document in schedule 1. This document lists the procedures the Council has in place to secure compliance with UK General Data Protection Regulation Article 5 when processing special category and criminal records personal data.

4. When we are:

    - processing personal data relying on one of the conditions in Articles 6 and 9 or 10 of UK General Data Protection Regulations;
    - processing personal data relying on a condition listed in the Data Protection Act 2018 parts 1, 2 or 3 of schedule 1;

    An Appropriate Policy Document applies.

5. Article 5 of the General Data Protection Regulation sets out the data protection principles. These are our procedures for ensuring that we comply with them.

Principle 1 – Lawfulness, Fairness and Transparency

We will:

- ensure that your personal information is only processed where there is a lawful basis to do so in Article 6 & 9;
- only process data fairly and make clear to the data subject what the information collected is being used for;
- ensure that data subjects receive information on how they can find out more information on how their personal information is being processed e.g., through privacy notices and retention schedules.

Principle 2 – Purpose Limitations

We will:

- only collect personal information for specified, explicit and legitimate purposes and will inform the data subject of these purposes in our privacy notices;
- not process personal information for any other purposes than specified in the collection of information.

Principle 3 – Data Minimisation

We will only collect the minimal personal information that is necessary to perform our tasks and will ensure information is adequate and relevant, data collected should be sufficient to properly fulfil the purposes it is required for and is limited to what is necessary. We periodically review the data we hold and delete anything we don't need.

Principle 4 – Accuracy

We will ensure individuals' personal information is accurate and, where necessary, kept up to date to ensure security.

Principle 5 – Storage Limitations

We will only keep personal data in identifiable form as long as is necessary for the purposes for which it is collected, or where we have a legal obligation to do so. Once we no longer need personal data it shall be disposed of confidentially.

Principle 6 – Integrity and confidentially

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Principle 7 – Accountability

The Council is responsible and will be able to demonstrate compliance with these principles.

The DPO is responsible for ensuring that the organisation is compliant with these principles:

- ensure that records are kept of all personal data processing activities, and that these can be provided to the Information Commissioner on request;
- carry out a Data Protection Impact Assessment for any high-risk personal data processing, and consult the Information Commissioner if appropriate;
- ensure that a DPO is appointed to provide independent advice and monitoring of the departments' personal data handling, and that this person has access to report to the highest management level of the department;
- have in place internal processes to ensure that personal data is only collected, used or handled in a way that is compliant with data protection legislation.

Retention and Erasure of Personal Data

6. The Council will ensure when processing special category information and criminal conviction personal information that it will be disposed of securely and confidentially.

7. Where we no longer require special category or criminal convictions personal data for the purpose for which it was collected, we will delete it, put it beyond use or render it permanently anonymous.

8. Data subjects receive full privacy information about how their data will be handled, and that this will include the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period. This information is set out on our website.

Review

9. We will review this policy from time to time and upon learning of any change to the law that affects the processing of special category data or criminal records data.