Thanet District Council

Data Protection Policy

Thanet District Council
Data Protection Policy

1.0 Introduction

1.1 Thanet District Council ("the Council") has a statutory duty to meets its obligations as set out within the context of the changes required by the General Data Protection Regulation ("GDPR")[1] and the Data Protection Act 2018 ("DPA"). 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 Relationship with other policies and procedures

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

- Data Minimisation Policy and Retention Schedules;
- Subject Access Request Procedure;
- Data Breach Procedure;
- Data Protection impact Assessment Procedure and Form (DPIA);
- Secure Working Environment Procedure;
- The Council's Privacy Statement and (general) Privacy Notice, along with specific Departmental Privacy Notices; and
- Corporate Compliance Statement (this is also what is called the "**Record of Processing Activities**" in the GDPR and this incorporates all Departmental Compliance Statements

2.0 Policy

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

2.2 Directors are responsible for ensuring all Council Personnel comply with this Data Protection Policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

2.3 The ICO is responsible for ensuring compliance with the GDPR; and has extensive powers under the 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.

2.4 Any breaches of the GDPR must be reported to the Data Protection Officer ("DPO").

2.5 The DPO has responsibility for data protection and for ensuring compliance with the law and will be the first point of contact for any cases of doubt.

[1] References to GDPR in this policy mean the General Data Protection Regulations 2016 (GDPR) as supplemented and varied by the Data Protection Act 2018.

2.6 The DPO can be contacted with questions about the operation of this policy, GDPR or on any concern about compliance with this policy. Some instances where the DPO can be contacted are:

(a) Where there is uncertainty about the lawful basis being relied on to process Personal Data (including where the Council uses legitimate interests);
(b) Where there is need to rely on Consent and/or need to capture Explicit Consent;
(c) To review and/or authenticate service area specific privacy notice;
(d) Ascertaining the retention period of personal data being processed;
(e) Uncertainty about what security or other measures is required to protect Personal Data;
(f) If there has been a (suspected)[2] personal data breach;
(g) To determine the basis (and legality) to transfer Personal Data outside the EEA;
(h) To render assistance in dealing with any rights invoked by a Data Subject;
(i) Where there is engagement in a significant new, or change in, processing activity which is likely to require a Data Protection Impact Assessment[3] (DPIA) or where there is a plan to use Personal Data for purposes others than what it was collected for;
(j) Where there is a plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making[4];
(k) Where help is required in complying with applicable law when carrying out direct marketing activities; or
(l) Where help is required with any contracts or other areas in relation to sharing Personal Data with third parties (including our contractors/consultants)

2.5 This policy covers, but is not limited to, personal data and special categories of personal data as defined by GDPR.

2.6 The Council will process data in line with the following 6 principles and the other requirements of GDPR as follows:

(a) Personal information will be obtained and processed fairly and lawfully and in a transparent manner in relation to individuals ('**lawfulness, fairness and transparency'**);
(b) It will be obtained and processed for specified purposes ('**purpose limitation'**);
(c) Personal information shall be adequate, relevant and not excessive in relation to the purpose for which it is processed ('**data minimisation'**);
(d) 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'**);
(e) 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 GDPR in order to safeguard the rights and freedoms of individuals ('**storage limitation'**); and

[2] Even if there is ambiguity about whether the data incident constitutes a breach, the DPO must be notified to make that judgement call.
[3] see further in the policy
[4] see further in the policy

(f) 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'**).

2.7 The GDPR also introduces a new accountability principle. This is an overarching requirement to objectively demonstrate compliance with all the above principles in the Regulation.[5]

3.0 Legal Definitions

3.1 The following definitions shall apply:

i. **Data Protection Legislation** means:
- General Data Protection Regulation ("GDPR"), which is directly applicable from 25 May 2018;
- Data Protection Act 2018 ("DPA") which main provisions are directly applicable from 25 May 2018;
- Law Enforcement Directive;
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 and Amendments ("E-Privacy Directive"); and
- Any other applicable law concerning the processing of personal data and privacy

ii. **Data** means information which:
- Is being processed wholly or partly by automated means,
- Is processed other than by automated means and forms part of a filing system i.e. structured set of data which are accessible by specific criteria,
- Is processed other than by automated means and is intended to form part of a filing system.

iii. **Personal data** means any information, which either directly or indirectly, relates to an identified or identifiable living individual. 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.

iv. **Special Category Data** means personal data consisting of information as to:
- The **racial or ethnic** origin of the data subject;
- **Political** opinions;
- **Religious** beliefs or other beliefs of a similar nature;
- Whether he/she is a member of a **trade union** (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
- **Physical** or **mental health** or condition;
- **Genetic** data;
- **Sexual life** and **sexual orientation**;
- **Biometric data** in order to uniquely identify a person ("biometric data" is information relating to individuals' physical or behavioural characteristics which allow unique identification of that individual, such as fingerprint recognition, voice recognition, facial recognition or walking pattern recognition)

[5] This accountability principle fundamentally mandate the Council to maintain an audit trail of all policies, procedures and any other indicators that show data protection compliance is genuinely embedded in its functions.

v. **Criminal Convictions Data** means personal data consisting of information as to:
- The commission or alleged commission by him/her of any offence; or
- Any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

vi. **Processing** in relation to information or data, means any operation(s) performed on personal data or sets or personal data (whether automated or not) such as collection, use, storage, dissemination and destruction.

vii. **Data subject** means an individual who is the subject of personal data.

viii. **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.

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

x. **Automated Decision-Making (ADM)** means when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

xi. **Automated Processing** refers to any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

xii. **(Explicit) Consent** means an agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

xiii. **Council** refers to Thanet District Council PO Box 9 Cecil Street Margate Kent CT9 1XZ, the Data Controller.

xiv. **Council Personnel** refers to all employees, workers, contractors, agency workers and consultants of the Council.

xv. **Members** refer to elected Councillors for the District of Thanet.

xvi. **Personal Data Breach** means any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that the Council or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

xvii. **Privacy by Design** means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

4.0 Roles and Responsibilities

4.1 The Council is responsible for ensuring that personal data is kept securely in the right hands and is accurate. However there are specific responsibilities allocated to certain individuals.

(a) **The Council** as a data controller shall ensure that:

- It is duly registered with 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 principles and that processing activities meet a lawful basis for processing;
- Staff processing personal data are appropriately trained to do so and continue to provide mandatory annual data protection training to these staff;
- All Staff are provided with appropriate data protection support and guidance.

(b) **Data Protection Officer (DPO)**

The Director of Corporate Governance 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;
- Developing policies and procedures, advising on DPIAs and conducting internal audits;
- Analysing all incidents, determining when a breach will be a breach[6], 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.

(c) **Senior Information Risk Owner (SIRO)**

This is the owner of information risk management at director level 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.

(d) **The Information Governance Manager (and Officer role**):
They are responsible for:

- Providing Information Governance (IG) support and guidance to the council to ensure that staffs are aware or their responsibilities and obligations in data protection;
- Providing mandatory data protection training to council staff;
- Ensuring that any queries about data protection, internal and external to the organisation are dealt with effectively;

[6] The DPO can also contact the ICO helpline in conflicting instances to clarify when a breach is a breach.

- Working across the council's functions to ensure there is consistency and application in data protection;
- Developing and regularly reviewing the council's IG policies and procedures;
- To facilitate information sharing between the council and other organisations by developing information sharing agreements when required.

(e) **Information Asset Owner (IAO)**

This is an individual appointed to ensure that specific information assets are handled and managed appropriately. IAO's are key decision makers across information they own in their relevant service areas.

(f) **Council Staff**

All persons to which this policy applies shall ensure they process information in line with data protection legislation. This includes complying with related policy requirements and undertaking mandatory annual Information Governance training.

5.0 Record of Processing Activity

5.1 The Council shall maintain a written record of its data processing activities. This will contain as a minimum the following information:

- our name and contact details, the name and contact details of our data protection officer (where applicable) and the names and contact details of any joint controllers (where applicable);
- the purposes of our processing;
- a description of the categories of individuals and of the categories of personal information we hold;
- the categories of recipients to whom the personal information have been or will be disclosed including recipients in third countries or international organisations;
- where applicable, transfers of personal information to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers which are necessary for the performance of a contract with the individual, the documentation of appropriate safeguards;
- where possible, the envisaged time limits for erasure of the different categories of personal information;
- where possible, a general description of the technical and organisational security measures taken to ensure the security of processing.

5.2 The Information Governance team shall be responsible for creating and maintaining the record of processing activity in conjunction with Information Asset Owners.

6.0 Privacy Notices

6.1 The Council shall ensure that a privacy notice is published on the council website. This shall:

- Explain in general terms the purposes for which the council will process the data collected;
- It shall explain where we keep information and why we hold it and for how long;
- It shall explain where we get personal data from and whom we share personal data with;
- It shall provide contact details of relevant staff to allow requests for further information;

- In certain circumstances, it shall be necessary for service areas to provide additional information, to that described, within their own privacy notice, for example when and where you might share personal data with others;
- A copy of the privacy notice shall be provided **on request and free of charge**.

7.0 Data Protection Impact Assessment (DPIA)

7.1 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 or system will affect the privacy of the individuals involved, while allowing the aims of the project to be met whenever possible.

7.2 We are also required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (e.g. Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles. A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

7.3 Staff shall consult with the Information Governance team at an early stage to identify DPIA requirements. The process to be followed shall be set out in a DPIA procedure and the Information Governance team will develop and provide adequate tools for conducting a DPIA.

7.4 The DPO shall be consulted on all DPIAs.

8.0 Data Security

8.1 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:

(a) Security policies and procedures shall be made available to all staff;
(b) The Council shall take all reasonable steps to adequately train all staff;
(c) The Council shall record and investigate all personal data breaches, led by the DPO;
(d) Where it is determined that a breach results in a 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;
(e) 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.

All applicable aspects of the Council's information Security, Risk and Governance Framework must be complied with, without attempting to circumvent the administrative, physical and technical safeguards the Council implements and maintains in accordance with the GDPR and relevant standards to protect Personal Data.

8.2 Payment Card Industry Data Security Standard PCI (DSS)

8.2.1 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.

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

8.4 Transfers to third parties

8.4.1 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[7], such transfers will only be completed in accordance with data protection legislation.

8.4.2 Approval in such circumstances will be made by a Senior Officer.

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

8.4.4 Information over the phone will only be given when the officer concerned is confident he or she knows to whom they are speaking and that disclosure is appropriate.

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

8.4.6 The Council will exercise particular care in relation to disclosure of special categories of personal 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.

9.0 Contracts

9.1 Contracts shall include measures to ensure personal data is handled in accordance with the data protection legislation following these guidelines:

- Personal data shall only be supplied for the agreed purposes as set out in the contract and shall not be used or disclosed for any other reason;
- The Council shall ensure that before personal data is shared with a third party as part of a contract, appropriate security controls are in place;
- There is a fully executed written contract that contains GDPR approved third party clauses has been obtained.

10.0 Information Sharing

10.1 The Council will take the following steps when sharing information with third parties, such as our service providers:

(a) The Council shall ensure that information is shared only when it is within the provisions of data protection legislation;
(b) The Council shall ensure that when information is shared it is justified and necessary to meet a lawful basis for processing as set out in this policy;
(c) The Council shall ensure sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

[7] This is not an exhaustive list. This Council maintain several privacy notices for specific services it implements. This Policy (in particular this point) must be read in conjunction with the relevant privacy notice which will disclose the exact third parties the Council may share an individual's data with, in order to carry out that exact service.

(d) The Council shall ensure that adequate security is in place to protect the data when it is shared with another organisation and that a fully executed written contract that contains GDPR approved third party clauses has been obtained;
(e) The council shall ensure the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
(f) The Council shall ensure the secure transfer of personal data between itself and other organisations;
(g) The Council shall ensure that the transfer complies with any applicable cross border transfer restrictions;
(h) The Council shall ensure that information sharing agreements exist between itself and partnership agencies such as the Kent and Medway Information Sharing Agreement.
(i) 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.

10.2 The Council recognises that it is important to state the types of purposes for which it will be legitimate to share personal information. We may share information for the following legitimate purposes:

- To provide direct health or social care to individuals, including mental healthcare;
- To maximise individuals' access to benefits;
- To support individuals in, or into, employment;
- To assist individuals with housing and enforce housing standards;
- To support individuals who are homeless;
- For reasons of environmental protection;
- To help individuals who have been identified as at risk, or who may be so identified;
- To address fuel poverty and water poverty;
- To provide counselling services;
- To safeguard vulnerable adults;
- To support vulnerable families;
- To safeguard children and young people;
- To support or improve educational provision;
- To detect, prevent or provide assistance in cases of domestic abuse;
- To enforce professional standards;
- To support the Prevent Strategy;
- To aid with the detection or prevention of crime;
- To support Liaison and Diversion Schemes;
- For reasons related to the detection and prevention of terrorism;
- To aid with the detection and prevention of non-criminal acts that are nevertheless unlawful;
- To address anti-social behaviour;
- To support release from custodial settings;
- To improve the efficiency of service provision;
- To improve operational efficiency;
- For reasons of public safety and emergency planning;
- To assist emergency responders;
- For research purposes;
- To calculate and levy tax and to investigate matters relating to tax;
- To combat fraud;

- For purposes of immigration control;
- For purposes related to inquests or investigations by Coroners;
- To facilitate reimbursement of costs or to apply charges for services.

The Council recognises that the type and extent of personal information which it is fair and lawful to share with thid parties will be different for each of the purposes set out above.

11.0 Individual Rights

11.1 Individuals have a right to view personal information about themselves and their family. They are entitled to know:

(a) What data is held or otherwise processed about them;
(b) The purpose of the processing;
(c) The recipients or categories of recipient to whom the personal data have or will be disclosed, in particular recipients in third countries or international organisations;
(d) Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
(e) The existence of the right to request from the controller (i.e. the Council) rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
(f) The right to lodge a complaint with the ICO;
(g) Where the personal data are not collected from the data subject, any available information as to their source;
(h) 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.

12.0 Lawful bases for processing personal information (personal and special category)

12.1 The Council will only collect and process personal data if one of the conditions set out in Article 6 of the GDPR have been satisfied. In all processing activities, you must have a valid lawful basis in order to process personal data. You must determine the lawful basis before you begin processing and this must be appropriately documented.

12.2 No single basis is 'better' or more important than the others; which basis is most appropriate will depend on the purpose for processing and the council's relationship with the individuals concerned. The appropriate bases for different services the Council renders are more specifically documented in the specific privacy notices for these service areas.

12.3 We have set out below each of the conditions under Article 6 of the GDPR that could be potentially relevant for the Council's activities:

There are **six** available lawful bases to the Council for processing Personal Data:

(a) **Public Task:** In many instances, the lawful basis relied on by the Council in the course of carrying out its primary duties will be that of processing of personal information required for the **performance of a public task**. This takes two forms:
    - The processing is necessary 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

- The processing is necessary 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).

The Council understands that in order to rely on the public task lawful basis, the processing must be strictly required in order for us to perform the relevant public task.

(b) **Legal Obligation**: The Council can process personal information where it is necessary in order for us **to comply with a legal obligation** to which we are subject. For us to rely on this basis, we must be bound by the legal obligation. This does not mean that there must be a legal obligation specifically requiring the processing, but our overall purpose must be to comply with a legal obligation. Notably, contractual obligations do not qualify as a legal obligation for these purposes.

(c) **Vital Interests:** We can process personal information where it is necessary in emergency situations or where the **vital interests** of the individual or another living person need to be protected.

"Vital interests" include protecting the life of a person, or protecting their bodily integrity. This is limited in scope and applies, for example, to life or death situations, or to contending with infectious diseases or humanitarian emergencies.

(d) **Contract:** We can process personal information where that processing is necessary for the performance of a contract with the data subject including specific steps before entering into a contract.

(e) **Legitimate Interests:** In some limited circumstances, we can process personal information for legitimate interests, which means we are happy to take full responsibility for justifying the processing because we are confident that we are protecting the interests of the data subject or we are acting in our own specific and compelling interests or in the specific and compelling interests of a third party.

As a **public authority**, the Council **cannot** rely on this basis for processing of personal information which is part of the performance of our public tasks. However, we can consider this basis where the processing of personal information is happening as a result of other legitimate purposes outside of our public tasks. It is generally preferable for public authorities to avoid this basis, so the circumstances where we can rely on it to process personal information will be very limited.

(f) **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.

The Council will therefore only **rarely use consent** as a lawful basis for processing personal information, and will only use it where we want to give individuals the ongoing power to decide whether their information is shared or not (e.g. for direct marketing).

12.4 Personal information, especially **special categories** personal information, about employees and members of the public is shared only with staff that needs to know the information in order to carry out their public task(s). This may involve sharing information between individuals in different departments. 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.

12.5 The Council will only collect and process special categories personal data if one of the conditions set out in Article 9 of the 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 GDPR. We have set out each of the conditions under Article 9 of the 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 GDPR**:

(a) **Explicit Consent**: freely given, informed and evidenced by a clear affirmative action;
(b) **Employment, social security or social protection law**: necessary to meet legal obligations in these specific areas
(c) **Vital Interests:** necessary to protect the life of the data subject or another individual where they are physically or legally incapable of giving consent;
(d) **Not-for-profit Bodies:** processing carried out by a political, philosophical, religious or trade union;
(e) **Deliberately made public by the Data Subject**: data that has manifestly been placed in the public domain by the Data Subject;
(f) **Legal Claims**: necessary for establishing, exercising or defending legal rights;
(g) **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;
(h) **Public interest in the area of Public Health**: such as threats to health or ensuring high standards of healthcare; and
(i) **Archiving Purposes**: public interest, scientific and historical research purposes or statistical purposes;
(j) **Substantial Public Interest:** necessary for reasons of substantial public interest such as for: official functions, administration of justice purposes, equal monitoring purposes, protecting the public against dishonesty, malpractice or other serious improper conduct purposes, preventing fraud, making certain disclosures under the Terrorism Act 2000 and the Proceeds of Crime Act 2002 or preventing or detecting unlawful acts including unlawful failure to act.

12.6 The current data protection legislation imposes stringent rules on the processing of **criminal allegations, convictions and offences, or related security measures**[8]**.** In the exceptional 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[9]; or acting in the vital interests of the data subject; or it is necessary for reasons of substantial public interest for the purpose of complying with the provisions of GDPR as

[8] Collectively referred to as 'criminal offence data'
[9] Part of the Crown and the processing is necessary for (i) any legal proceedings; (ii) obtaining legal advice; or (iii) establishing, exercising or defending legal rights.

supplemented by the Data Protection Act 2018 (DPA) and having an appropriate policy document[10] in place. This is in addition to first, a lawful basis for processing under Article 6 of the GDPR.

12.7 The Council will retain[11] criminal offence data for the duration of 7 years after the relationship of the Council to the data subject has ended before erasing the data. In some instances, criminal offence data may be kept for longer than 7 years subject to legal considerations involving the nature of the conviction, the relationship of the data subject with the Council and where the Council has determined it is in the best interests of the public to do so.

13.0 Children

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

13.2 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, we balance the public's interests in processing the personal data against the interest and fundamental rights and freedoms of the child.

13.3 When relying on consent, the Council will ensure it makes reasonable efforts to verify children are aged 13 and above to give a valid consent. In addition, we will also make sure that the child understands what they are consenting to.

13.4 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.

13.5 Wherever the Council is offering a service to a child under the age of consent which is 13 in the UK by virtue of the DPA 2018; we 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.

13.6 Generally, Children have the same rights as adults under 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.

13.7 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.

13.8 Where a child exercises their right to erasure where we rely on 'consent' or 'legitimate interests' to process their data, the Council will give particular credence in acceding to this

[10] This Policy (data protection policy) is our "appropriate policy document" for the purpose of the Council processing Criminal offence data, and it explains how we comply with data protection principles, retention and erasure of personal information; and that it will be reviewed regularly.

[11] The DPA 2018 [Part 2, para. 5 (1&2) and para. 6(1&2)] supplements the GDPR by providing the legal basis for processing criminal convictions and offences. In the Council's case, as a 'public authority' and when it is in the public interest to do so. Part 4, para. 39-41 of the DPA stipulates additional safeguards to processing this data to include having a policy that states the retention period and erasure of criminal conviction data.

request. And this applies even when the data subject is no longer a child, as they might not have been aware of the risks involved in processing at the time of consent.

13.8 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.

14.0 Accountability

14.1 The Council will implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles.

14.2 There will be adequate resources and controls in place to ensure and to document GDPR compliance including:

(a) appointing a suitably qualified DPO who reports to an executive board of management;
(b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;
(c) integrating data protection into internal documents including data protection related policies and procedures, information security risk and governance framework, and Privacy Notices;
(d) regularly train Council Personnel and Members on general data protection, GDPR, related policies and data protection matters including, for example, Data Subject's rights, Consent, lawful bases, DPIA and Data Breaches. The record of training attendance will be maintained; and
(e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

14.3 All personnel must undergo all mandatory data privacy related training in accordance with the Council's corporate training programme.

14.4 There will be regular review of all the systems and processes to ensure they comply with this Policy; particularly that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

15.1 Right related to Automated Processing (Including Profiling) and Automated Decision-Making (ADM)

15.1.1 Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

(a) a Data Subject has Explicitly Consented;
(b) the Processing is authorised by law; or
(c) the Processing is necessary for the performance of or entering into a contract.

15.1.2 If certain types of Special Categories of Personal Data or Criminal Convictions Data are being processed, then grounds (b) or (c) above will not be allowed but such Special Categories of Personal Data and Criminal Convictions Data can be processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

15.1.3 If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed when we first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

15.1.4 We will also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

15.1.5 A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

15.2 Direct Marketing

15.2.1 We are subject to certain rules and privacy laws when marketing to our customers.

15.2.2 For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as 'soft opt in' allows us to send marketing texts or emails if we have obtained contact details in the course of a service transaction to that person, we are marketing similar services, and we gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

15.2.3 The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

15.2.4 A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

16.0 Right of Access to Personal Information

16.1 In addition to their rights under this policy, all of the Council's employees, and members of the public in respect of whom personal data is processed have a right to ask the Council, under the GDPR, for personal information held about them and this section details the information they are entitled to see under the GDPR.

16.2 These rights under the GDPR are stated thus:

- Within one calendar month of **a written request and free of charge**, a data subject is entitled to:-
- Be told whether personal data, of which he or she is 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 object to processing; 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.

17.0 Access to Personal Information Refused

17.1 The Council reserves the right to refuse the employee or requester access to information if:

- It would identify another individual/organisation that has not consented to the disclosure. It is important to note that organisations are not covered by GDPR 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

18.0 Objection to processing

18.1 Individuals have the right to object to processing by the Council's for the performance of a task in the public interest and/or their exercise of official authority. In these instances, where an individual objects, the Council must stop processing the personal data unless:

- We 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.

19.2 Withdrawal of consent

19.1 An individual has the right to withdraw consent at any time.

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

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

19.4 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.

20.0 Right to Erasure ("right to be forgotten")

20.1 Furthermore, a data subject has a right to ask the Council, under the GDPR, for their personal information to be erased under GDPR.

20.2 Barring any exception, this request must be actioned within **one calendar month of a written request and usually free of charge** except where the request is manifestly unfounded or excessive, then we may charge a reasonable fee for the administrative costs of complying with the request**.**

20.3 This right to erasure **does not** apply where the Council is processing Data subjects' personal information when it is exercising its right to freedom of expression and information; and whilst processing under the following lawful bases as specified in the GDPR:

- for the performance of a task carried out in the public interest or in the exercise of official authority;
- to comply with a legal obligation;
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims.

20.4 The Council **has** to comply with an individual's request to have their personal data erased or deleted where any one or more of the following applies:

- the personal data is no longer necessary for the purpose which we originally collected or processed it for;
- we are relying on consent as your lawful basis for holding the data, and the individual (or children) withdraws their consent;
- we are relying on legitimate interests as our basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- we are processing the personal data for direct marketing purposes and the individual objects to that processing;
- we have processed the personal data unlawfully;
- we have to erase their data in order to comply with a legal obligation; or
- we have processed the personal data to offer information society services to a child.

20.5 Once it has been established that the 'right to erasure' applies; we will notify others about the erasure of personal data:

(a) Where we have disclosed the personal data to third parties[12], we must contact each recipient notifying them of the erasure unless this proves impossible or involves disproportionate effort. And if requested, we must tell the data subjects about these recipients; and
(b) Where personal data has been made public in an online environment, the Council will take reasonable steps to inform other controllers/processors who are processing the personal data to erase links to, copies or replication of that data.

21.0 CCTV

21.1 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.

21.2 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.

21.3 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.

21.4 The Council will ensure that clear notices are in place identifying when an individual is entering into 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.

21.5 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.

21.6 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 the Council's Information Sharing Policy.

22.0 International Transfers

[12] The GDPR defines a recipient as a natural or legal person, public authority, agency or other body to which the personal data are disclosed. The definition includes controllers, processors and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

22.1 The Council shall not transfer personal data outside the European Union, to 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.

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

22.3 Any systematic sharing of personal data outside of the UK shall be subject to a DPIA.

23.0 Equality & Diversity

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

24.0 Compliance with this Policy

24.1 The Council recognises that compliance with this policy is important. Breach of data protection law can result in commission of a criminal offence. In particular, knowingly obtaining or disclosing personal data without the consent of the Council is an offence.

24.2 This Data Protection Policy applies to all Council Personnel and Members. They must read, understand and comply with this Data Protection Policy when Processing Personal Data on the Council's behalf and attend training on its requirements. This Data Protection Policy sets out what is expected from all in order for the Council to comply with applicable law. Compliance with this Data Protection Policy is **mandatory**. All Personnel and members must comply with all Related Policies and Privacy Guidelines which are available to help them interpret and act in accordance with this Data Protection Policy.

24.3 It is the policy of the Council to consider disciplinary proceedings for any staff that breach this policy; and termination of contract for agency workers, contractors and consultants.

25.4 Any breach of this Data Protection Policy by Members will be regarded as a breach of the Council's Code of Conduct for Members. And any Member who discloses personal information held by the Council for their own personal use or the use of their political party for electioneering purposes without our consent is likely to have committed an offence.

24.5 Whenever a staff or member have a specific responsibility in connection with Processing personal information such as capturing Consent, reporting a Personal Data Breach, conducting a DPIA as referenced in this Data Protection Policy or otherwise, then they must comply with the Related Policies and Privacy Guidelines

25.0 Information Commissioner's Office

25.1 The Information Commissioner's Office (ICO) is the primary supervisory body for data protection. Notably, the ICO has greater enforcement and sanctions powers under the 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.

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

25.3 The Council shall 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.

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

26.0 Policy Review

26.1 This policy remains a live document, subject to ongoing reviews to ensure it continues to align with the requirements of relevant legislations.