WEST OXFORDSHIRE
DISTRICT COUNCIL

Data Protection Policy

Document Control

Version	Date	Author	Comments
1	January 2018	DPO	Compliance with new GDPR Legislation
2	October 2021	DPO	Compliance with regulation updates
3	September 2022	DPO	Regulation update
4	April 2026	DPO	IC Compliance update

Contents

1.0 Introduction

1.1 West Oxfordshire District Council ("the Council") has statutory duties under Data Protection Legislation to ensure the lawful, fair and secure Processing of Personal Data.

1.2 Information held by the Council is a valuable asset and we owe a duty of care to members of the public and to those who work for the Council, to protect their Personal Data from accidental or deliberate damage, disclosure, unauthorised modification or destruction.

1.3 This document sets out the Council's policy on data protection, affirming individuals' rights provided for under current Data Protection Legislation and setting out the responsibilities of those who work with Personal Data.

1.4 This policy applies to all Personal Data processed by the Council, regardless of format and to any individual Processing Personal Data held by the Council.

1.5 The Council states that, in general:

- It does not seek to offer goods or services to Data Subjects in the European Union.
- It does not seek to monitor behaviour which occurs within the European Union.
- Therefore, the EU General Data Protection Regulation 2016 does not apply to the Council.
- The Processing of Personal Data undertaken by the Council is carried out under UK Data Protection Legislation, including the Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR), the Law Enforcement Processing regime, the Privacy and Electronic Communications Regulations 2003 and the Data (Use and Access) Act.

2.0 Relationship With Other Policies and Procedures

2.1 This policy is underpinned and supplemented by a range of related policies, procedures and supporting documents within the Council. These include:

- Artificial Intelligence Policy
- CCTV and Body Worn Cameras Policy
- Corporate Retention Policy
- ICT Acceptable Use Policy
- Personal Data Breach Procedure
- Subject Access Request Procedure
- Data Protection Impact Assessments (DPIAs)
- The Council's service specific Privacy Notices
- Record of Processing Activities (ROPA)
- Business Continuity Plans

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 Information Commission (IC) is responsible for ensuring compliance with Data Protection Legislation and has extensive powers under the UK GDPR to take action against organisations that breach data protection law. The IC replaced the former Information Commissioner's Office (ICO) following governance reforms introduced by the Data (Use and Access) Act 2025.

3.3 Any breaches of Data Protection Legislation must be reported to the Data Protection Officer ("DPO") and Compliance and Information Governance team in accordance with the Council's Personal Data 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 Under the UK GDPR, the Council must comply with six data protection principles, which are summarised below:

- 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 it is processed, ensuring it is erased or rectified without delay when inaccuracies are identified (**'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 is processed solely for:
    - archiving purposes in the public interest,
    - scientific or historical research purposes,
    - statistical purposes,

  and subject to the implementation of the appropriate technical and organisational measures required by the UK GDPR to safeguard the rights and freedoms of individuals ('**storage limitation**').
- 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, which requires organisations be able to demonstrate compliance with all of the above principles.

4.0 Legal Definitions

4.1 The following definitions shall apply:

4.1.1 Data Protection Legislation means:

- The UK General Data Protection Regulation ("UK GDPR"),
- Data Protection Act 2018 ("DPA") - This was formerly the Data Protection Act 1988

- Law Enforcement Processing (DPA Part 3);
- The Privacy and Electronic Communications (EC Directive) Regulations 2003; and
- The Data (Use and Access) Act 2025 (DUAA 2025) received Royal Assent on June 19, 2025, marking its official passage into law.
- Any other applicable law concerning the Processing of Personal Data and privacy.

4.1.2 **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.

4.1.3 **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 individual's 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.

4.1.4 **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.

4.1.5 **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 and recording.
- Organisation and structuring.
- Storage, adaptation or alteration.
- Retrieval, consultation and use.
- Disclosure by transmission, dissemination or otherwise making available.
- Alignment or combination.
- Restriction.
- Erasure or destruction.

4.1.6 **Data Subject** means an individual who is the subject of Personal Data.

4.1.7 **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.

4.1.8 **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. While these obligations apply to the organisation as a whole, specific roles within the Council have defined responsibilities for supporting compliance.

5.1.1 The Council shall ensure that:

- It pays its registration fees annually to the Information Commission; our registration reference is Z6172644.
- 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 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.

5.1.2 The **Data Protection Officer** is a statutory appointed officer responsible for supporting the Council in meeting its obligations under Data Protection Legislation. The DPO is responsible 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 and reviews.
- Analysing all incidents, determining when a breach constitutes a Personal Data breach and reporting to regulatory authorities where applicable.
- Acting as the single point of contact for all Data Subjects.
- Acting as the single point of contact for the Information Commission and any other bodies engaged in the application of Data Protection Legislation.

The Council will support the DPO by providing the resources needed to undertake their tasks and access to Personal Data, processes and operations and by enabling the DPO to maintain their expert knowledge. The DPO must be able to perform their duties independently and the Council will not instruct the DPO on how they exercise their role.

5.1.3 The **Director of Place** is the Senior Information Risk Owner (SIRO), 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. The SIRO 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.

5.1.4 The Council's **Information Governance Manager (and Officer)** support the DPO and the Council in ensuring compliance with Data Protection Legislation and in implementing, developing and maintaining the Council's information governance arrangements in relation to UK GDPR, the Freedom of Information Act and complaints handling. These roles' responsibilities include but are not limited to:

- Providing Information Governance and Data Protection advice to all officers and services of the Council.
- Developing and maintaining information governance policies.
- Promoting data protection across the organisation to embed a strong data protection culture.
- Develop, implementing and maintaining guidelines, training and associated materials to help identify, manage, monitor and report on data protection risks.
- Review and identify legislation relevant to data Processing and information sharing and advising on the appropriate legal gateways.
- Identifying, reviewing, mitigating and eliminating risks of Personal Data breaches to individuals and risks to the Council (organisational and reputational).
- Reporting on data protection activities to the Corporate Management Team, highlighted data protection risks and training needs.
- Cooperating with the supervisory authority, including determining breach notification requirements.
- Advising on data protection relating to Subject Access Requests (SARs), Freedom of Information requests (FOIs) and Rights requests.
- Reviewing organisation and security risk for removable media and working arrangements.
- Working with services to complete Data Protection Impact Assessments (DPIAs).
- Creating, implementing and maintaining privacy notices, retention schedules and Records of Processing Activity with services.
- Undertaking data protection service audits.
- Responding to UK GDPR "rights" requests.

5.1.5 All **Council staff and Councillors** shall ensure they process personal 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 (ROPA)

6.1 The Council shall create maintain a written record of its data Processing activities (ROPA).

6.2 The Information Governance team, working with each department, shall be responsible for maintaining the Council's ROPA in accordance with Article 30 of the UK GDPR. Departments must notify the Information Governance team of any changes to their Processing activities during the review cycle to ensure the ROPA remains accurate and up to date.

6.3 The Council's ROPA

7.0 Privacy Notices

7.1 The Council will ensure that privacy notices are published on the Council's website. Each privacy notice will:

- 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.
- Explain the rights available to Data Subjects under UK GDPR (Articles 12–22).
- Make Data Subjects aware that they have the right to lodge a complaint with a supervisory authority.
- Explain where the Council keeps information, why it is held and for how long.
- Explain where the Council gets Personal Data from and with whom it shares it.
- Provide contact details for the DPO, to allow requests for further information.

7.2 If a service starts Processing Personal Data in a way that is not already covered by its privacy notice, it must provide additional privacy information to individuals, or create a project-specific privacy notice as appropriate.

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:

- Service specific privacy notices.
- Council form privacy statements.
- Just in time notices.

8.0 Data Protection Impact Assessments (DPIA)

8.1 The Council will complete a DPIA in the early stages of any project that involves high-risk Processing of Personal Data e.g. large-scale Processing, systematic monitoring or Processing Special Category Data. A DPIA will enable the Council to systematically and thoroughly analyse how a project, Processing activity or system will affect the privacy of the individuals involved and helps to identify and manage privacy risks.

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

8.3 The DPO shall be consulted on all DPIAs and will approve all DPIAs prior to commencement of Personal Data Processing.

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.

9.2 ICT Security policies and procedures shall be made available to all staff.

9.3 The Council shall take all reasonable steps to adequately train all staff.

9.4 The Council shall record and investigate all Personal Data and cyber security breaches (Personal Data breaches investigations are led by the Compliance and Information Governance team and overseen by the DPO and Senior Management when required).

9.5 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 Commission (IC) within 72 hours of becoming aware.

9.6 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 or Cyber Security Breach

10.1 Data Protection Legislation requires the Council to notify Personal Data and cyber security breaches that present a high risk to the rights and freedoms of Data Subjects, in certain instances, to the IC and affected Data Subject(s). Notifications will be made by the DPO; staff and Councillors **must not** attempt to notify the Data Subject or the IC.

10.2 The Council has procedures for dealing with any suspected Personal Data or cyber security breaches and will notify Data Subjects or the IC 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 or Compliance and Information Governance team by reporting it as a Personal Data or cyber security breach at:

- Report a Personal Data Breach: data.protection@westoxon.gov.uk
- Report a Cyber Security Breach: cyber.security@publicagroup.uk

10.4 Once the breach has been assessed, if high risk, a report will be made to the DPO and SIRO. If the breach relates to a cyber security incident the Head of Cyber Security Lead will also be sent the report. They will be in contact to review and investigate the report 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.

11.3 The Council has a PCI DSS Policy that sets out how the Council and its staff will comply with these standards.

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 know who they are speaking to and that disclosure is appropriate.

12.5 The Council will exercise particular care when disclosing special category Personal Data and Criminal Offence Data and will only disclose such data to third parties in limited circumstances, normally only where this is necessary for the Council to fulfil its statutory obligations or where disclosure is required to investigate crime and non-disclosure would prejudice the investigation (e.g., disclosure to the police).

13.0 International Transfers

13.1 The Council shall not transfer Personal Data to a third country or to international organisations unless there is a legal requirement to do so, the country has received a UK adequacy decision, or it can be evidenced that appropriate safeguards are in place as required by Data Protection Legislation.

13.2 Any data Processing or sharing of Personal Data outside of the UK should only be undertaken in accordance with IC guidelines with approval from the DPO.

14.0 Contracts

14.1 Contracts shall include measures to ensure Personal Data is handled in accordance with Data Protection Legislation and the Procurement Act 2023, 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 any Personal Data is shared with a third party under a contract, 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 Article 28 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 Compliance and Information Governance team and DPO shall provide the Council with guidance on information sharing, both systematic, long-term sharing and sharing in ad-hoc, one off circumstances.

15.2 Information Sharing may be conducted under the Oxfordshire Safeguarding Children Board (OSCB) framework.

- The OSCB is a high-level agreement between Oxfordshire local authorities and a number of public organisations in Oxfordshire. Its aim is to facilitate more effective data sharing across Oxfordshire.
- The Council is a signatory 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 OSCB 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:

- The organisations involved in the sharing.
- The Personal Data being shared (e.g., personal, special category, or Criminal Offence Data).
- The purpose for sharing.
- The legal gateway relied upon to enable the lawful sharing of information.
- The 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 IC.

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,** set out below:

(these are also known as lawful basis):

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 as a District Council (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 Notice.

17.4 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 of action than sharing personal information is available, then we should adopt the less invasive course. The Council must identify and document the legal grounds being relied on for each Processing activity.

17.5 The Council will only collect and process Personal Data where one or more of the lawful basis' set out in Article 6 of the UK GDPR (listed above in 17.3). The lawful basis for each activity must be identified and appropriately documented.

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 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, ensuring that only those people who have a need to know are able to access the Personal Data of a Data Subject.

17.8 The Council will only collect and process special category Personal Data if one of the conditions in Article 9 of the UK GDPR (listed below), or a relevant condition in Schedule 1 of the Data Protection Act 2018, has been satisfied. This is in addition to identifying a lawful basis under Article 6 (see 17.3).

- **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 organisation.
- **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 for preventative or occupational medicine, assessing the working capacity of an employee, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems.
- **Public Interest in the Area of Public Health:** such as managing threats to health or ensuring high standards of healthcare.
- **Archiving Purposes:** necessary for archiving in the public interest, scientific or historical research, 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. 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 take reasonable steps to verify that a child is capable of giving valid consent and that they understand what they are consenting to.

18.4 Where the child is not capable of understanding what they are consenting to, the Council will obtain consent from the person who holds parental responsibility. The Council will take reasonable steps to verify that the individual giving consent does indeed have parental responsibility for the child.

18.5 When relying on the lawful basis of 'performance of a contract', the Council will assess whether the child has the capacity to understand the agreement and to enter into a contract.

18.6 When relying on the lawful basis of 'public interest', including where this involves providing services the Council is under a statutory duty to deliver, the Council will balance the public interest in Processing the Personal Data against the child's interests and their fundamental rights and freedoms.

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 would 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 that Processing. The Council will also, where possible, seek to rely on other lawful bases aside from consent when Processing children's information.

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 The Council will ensure that requests for access to Personal Data are handled in accordance with statutory requirements and processed in a timely, fair and transparent manner.

19.3 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
- Be 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 IC.
- Be informed of the existence of any automated decision-making, including profiling and in such cases, be given meaningful information about the logic involved and the significance and envisaged consequences of the 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 where providing access would adversely affect the rights and freedoms of others or where a statutory exemption applies. Examples include where:

- Disclosure would identify another individual or organisation who has not consented and it would not be reasonable to disclose the information without their consent.
- The Council has reasonable doubt about the requester's identity and the requester has failed to provide appropriate identification following a request for verification.
- The information concerns an organisation rather than an individual. Organisations are not covered by Data Protection Legislation, however, to avoid any breach of personal confidentiality, the Council should seek consent before disclosure (unless it cannot reasonably be obtained and disclosure is otherwise justified).
- The information is legally privileged.
- The information consists of confidential employment references, given or to be given by the Council, relating to:
    - the education, training or employment of the worker;
    - the appointment of the worker to any office; or
    - the provision by the worker of any service.
- Disclosure would likely prejudice crime and taxation matters, including:
    - the prevention or detection of crime;
    - the apprehension or prosecution of offenders; or
    - the assessment or collection of any tax duty or 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 and disclosure would be an unjustified breach of confidence.
- Disclosure would, in the opinion of the Council or an appropriate health professional, be likely to cause serious harm to the physical or mental health of the requester or another individual.

  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 the Council's Processing of their Personal Data where the Council is relying on the lawful basis of performing a task in the public interest and/or exercising official authority. The same rights apply where the Council relies upon legitimate interest as its lawful basis when not acting as a public authority. In these instances, where an individual objects, the Council must stop Processing the Personal Data unless:

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

22.0 Withdrawal of Consent

22.1 An individual has the right to withdraw their consent at any time. It must be as easy to withdraw consent as it was to give it.

22.2 Where Personal Data is being processed solely on the basis of consent, the Processing must stop once consent is withdrawn.

22.3 If the Council has another lawful basis for Processing the Personal Data, such as public task or legal obligation, it may continue to process the data on that alternative basis, even after consent is withdrawn.

22.4 In practice a withdrawal of consent is likely to be accompanied by a request for erasure. In such cases, the Council must consider whether an exemption to erasure applies, for example where there is an overriding public interest or a legal obligation to retain the data.

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 under Data Protection Legislation as any other recorded information.

23.2 Each CCTV system has 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 and apprehension of offenders.
- Managing on-site traffic and car parks.
- Monitoring traffic movements.
- Protecting Council property and assets.
- Assisting in the investigation of incidents occurring on Council premises or land.
- Supporting the investigation and resolution of incidents, including those raised through complaints or formal 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 its use.

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. Notices 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 can exercise their rights in relation to any Personal Data about them that has been recorded on CCTV. 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 of this policy 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. A breach of data protection law can amount to a criminal offence, particularly where an individual, without lawful authority, knowingly or maliciously obtains, accesses or discloses Personal Data.

25.2 The Council may take disciplinary action against any member of staff who breaches this policy.

26.0 Information Commission

26.1 The Information Commission (IC), previously known as the Information Commissioner’s Office, is the UK’s supervisory authority for data protection. The IC oversees compliance with data protection law and has statutory powers to investigate concerns, issue guidance and take enforcement action where necessary.

26.2 The Council will comply fully with all requests from the IC 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 IC 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 Councillors may use Personal Data in three different capacities:

- When carrying out Council business (for example, in committees or working groups, considering issues and making decisions). In these circumstances, **the Council** is the data Controller.
- When acting as a member of a political party, such as when canvassing or working for a political party. In these circumstances, **the political party** is the data Controller.
- When undertaking casework on behalf of individuals. In this situation **the Councillor** is the data Controller.

27.2 When representing a constituent who has made a complaint or requested assistance, the Councillor's lawful basis for Processing Personal Data is the performance of a task carried out in the public interest.

27.3 Where sensitive (special category) information is processed, this is under the substantial public interest condition in Schedule 1, Part 2 of the Data Protection Act 2018 ("elected representatives responding to requests"). The Council will not generally rely on consent in these circumstances.

27.4 In representing their constituents, Councillors may need to share personal information with the Council, other Councillors and the Member of Parliament.

27.5 Personal information held by the Council must not be used by Councillors for political or party-related purposes.

27.6 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 obtained through their role as a representative of residents, such as complaints casework, should not be used without the explicit consent of the individual.

27.7 Councillors must take appropriate security measures to protect their constituents' personal information. They must take into account the sensitivity of the information and the potential harm to individuals that could result from unauthorised access or disclosure. Appropriate measures may include secure passwords, restricted device access and adherence to Council procedures and training.

27.8 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 Use of AI

28.1 The use of Artificial Intelligence (AI) may offer benefits to the Council by supporting new ways of working.

28.2 When considering its use, the Council should always ask: "What are we using it for?", "Does it do the job well?" and "What problem does it solve?".

28.3 The Council must also ensure it meets its legal obligations under data protection laws.

28.4 Currently, due to the risk of non-compliance with these laws, any information classified as restricted or highly restricted must not be submitted to generative AI tools (such as ChatGPT). This also includes sensitive non personal information, such as commercially sensitive data.

28.5 Data protection laws require all organisations to comply with a set of principles. The most relevant to the use of AI are summarised below, along with the issues they present:

- **Lawfulness, fairness and transparency:** Individuals must be made aware of how their data is being used, for what purposes and to whom it may being disclosed. AI tools can make this difficult, or in some cases impossible, as it may not always be clear how Personal Data will be processed or who may have access to it. The Council has an AI Privacy Notice in place to support this requirement.

- **Purpose limitation:** Personal Data must be collected for specified, explicit and legitimate purposes and must not be used for purposes that are incompatible with those original purposes. Submitting Personal Data to AI tools is likely to involve disclosure to a third-party provider, even if the provider states the data will be deleted after use.
- **Individual rights:** Individuals have rights regarding their Personal Data, such as the right to know who controls it, the right of access, the right to request erasure and the right to object to Processing. AI tools may make these rights harder to exercise, particularly where the data is disclosed to third-party providers or used in opaque Processing.
- **Fairness and the ability to exercise rights**: Where Personal Data is processed within AI tools, exercising these rights can be very difficult, particularly if individuals have no way of knowing where or how their Personal Data is being used. This may prevent individuals from effectively exercising their right and can be particularly concerning where AI tools produce biased or unfair outcomes, or where individuals lack a meaningful way to challenge decisions made using their data.

29.0 Policy Compliance

29.1 All staff, Councillors and contractors must comply with this policy and with any procedures or guidance issued to support it.

29.2 Staff, Councillors and contractors who are unsure about the implications of this policy, or how it applies to their role, must seek advice from the Data Protection Officer (DPO).

29.3 This policy will be reviewed regularly and updated as necessary, including when changes in legislation, guidance or organisational practice affect how the Council processes Personal Data.

Appendix 1 Appropriate Policy Document

Processing Special Category Data and Criminal Records Data

1. This Appropriate Policy Document sets out the Council's procedures when processing special category Personal Data and criminal records Personal Data.

2. Special Category Data and criminal records data are both forms of Personal Data that warrant additional safeguards due to their sensitivity. This policy document provides assurance of those safeguards and outlines the requirements under Data Protection Legislation.

3. Schedule 1 of The Data Protection Act 2018 sets out the requirements for an Appropriate Policy Document. This document lists the procedures the Council has in place to ensure compliance with UK General Data Protection Regulation Article 5 when processing special category and criminal records Personal Data.

4. An Appropriate Policy Document applies when the Council is:

    - Processing Personal Data relying on one of the conditions in Articles 6, 9 or 10 of UK General Data Protection Regulations; or

    - Processing Personal Data relying on a condition listed in the Data Protection Act 2018 parts 1, 2 or 3 of schedule 1.

5. Article 5 of the UK GDPR sets out the data protection principles. The Council's procedures for complying with these principles are as follows.

Principle 1 – Lawfulness, Fairness and Transparency

We will:

- Ensure that personal information is only processed where there is a lawful basis to do so under Articles 6 and (where applicable) 9.
- Process data fairly and make clear to Data Subjects what the information collected will be used for.
- Provide Data Subjects with clear privacy information (e.g., via 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 purposes that are incompatible with the original purposes of collection.

Principle 3 – Data Minimisation

We will:

- Only collect the minimum personal information necessary to perform our tasks.
- Ensure data collected is adequate and relevant to the stated purpose.
- Periodically review the data we hold and delete anything that is no longer required.

Principle 4 – Accuracy

We will:

- Take reasonable steps to ensure personal information is accurate and, where necessary, kept up to date.
- Rectify or erase inaccurate personal information without undue delay.

Principle 5 – Storage Limitations

We will:

- Retain Personal Data in identifiable form only 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

We will:

- Protect Personal Data against unauthorised or unlawful Processing and against accidental loss, destruction or damage.
- Implement appropriate technical or organisational measures to secure data (e.g., access controls, encryption, secure transfer, training and governance) proportionate to the risks.

Principle 7 – Accountability

We will:

- Be responsible for and will be able to demonstrate, compliance with these principles.
- Ensure that records are kept of all Personal Data Processing activities and that these can be provided to the Information Commission on request.
- Complete Data Protection Impact Assessments for any high-risk Personal Data Processing and consult the Information Commission where appropriate.
- Ensure that a Data Protection Officer (DPO) is appointed to provide independent advice and monitor Personal Data handling, with access to the highest level of senior and service management.
- Maintain internal processes to ensure that Personal Data is only collected, used and handled in a way that is compliant with Data Protection Legislation.

Retention and Erasure of Personal Data

We will:

- ensure that special category and criminal convictions Personal Data are retained only for as long as necessary and, when no longer required, securely erased, put beyond use, or rendered permanently anonymous.
- Provide Data Subjects with privacy information that includes retention periods (or the criteria used to determine them), as set out on the Council's website.
- Follow the Council's Data Retention Policy, which defines how long data is retained, where it is stored and when it is securely deleted, ensuring compliance and reducing risk.

Review

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.