Data Protection Policy 2026

Document Author:	Richard Steele CIPM, Group IG Manager and DPO
Document Approved:	SHDC BBC ELDC
Document Review date:	

1. Introduction

This document ("Policy") outlines how ("the Council", "we", "our", "us") handles personal data, protecting individuals' privacy under the:

- UK General Data Protection Regulation (UK GDPR) 2018
- Data Protection Act 2018 (DPA 2018)
- Privacy and Electronic Communications Act 2018 (modified GDPR)
- Human Rights Act 1998 (Article 8)
- Data (Use and Access) Act 2025 (DUAA)
- And guidance from the Information Commissioner's Office (ICO).

It applies to all staff, elected members, contractors, agency staff, consultants, and partners.

2. Scope

This Policy applies to all personal data in all formats (electronic, paper, audio, etc.) held by or on behalf of the Council and to all individuals or organisations processing this data.

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

This policy supports our other policies. We may supplement or amend this policy by additional policies and guidelines from time to time.

3. Data Protection Principles

We are committed to the seven UK GDPR principles:

1. **Lawfulness, fairness & transparency** – process data legally and openly.
2. **Purpose limitation** – collect only for specified, explicit reasons.
3. **Data minimisation** – gather only what is necessary.
4. **Accuracy** – maintain data accuracy and timeliness.
5. **Storage limitation** – retain only as long as required.
6. **Integrity & confidentiality** – protect data with safeguards.
7. **Accountability** – show compliance clearly.

We commit to the DUAA specific commitments:

- Enabling **lawful access & reuse** of public-sector datasets.
- Ensuring **interoperability** and **transparency** in data sharing.

4. Roles and Responsibilities

Each Council is designated "Data Controller" for the data it generates, uses and accesses in delivery of its public task.

Senior Information Risk Owner (SIRO): Strategic oversight.
Data Protection Officer (DPO): Compliance monitoring, advice, liaison.
Managers/Service Leads: Operational enforcement.
All Staff & Members: Must follow this Policy and report concerns promptly.

Members may be a Data Controller for personal information not covered by this Data Protection Policy where that processing is for political, personal or casework. (this is expanded in Appendix G)

5. Rights of Individuals

Each person has a right to know that the Council is using, storing and sharing their information in a clear and transparent way. There are provisions within the Data Protection Act known as 'subject's rights' that an individual can use to see, amend and challenge the use of their information. This is known as a "subject access request" or a "SAR". All SARs must be directed to the DPO for co-ordination. (this is expanded in Appendix A)

In some cases the Council uses information to meet a lawful obligation placed upon it by a series of legislation. If this is the case the Council may need to withhold some of the 'subject's rights'.

Individuals have the right to request:

- Access their personal data.
- Correct errors.
- Request erasure ("right to be forgotten").
- Restrict or object to processing.
- Data portability (move information to another organisation).
- Withdraw consent.
- Challenge automated decisions.
- Lodge complaints with the Council and the ICO

Under DUAA, we also ensure transparency about who accesses and reuses public data.

6. Data Sharing and Access

Data will only be shared under a valid legal basis, supported by contracts or Information Sharing Agreements (ISAs).

Per DUAA, we mandate:

- Lawful access to datasets where required.
- Use of interoperable formats.
- A transparency register of accessed/shared data.

All data sharing must be documented and risk assessed by the DPO, approval for processing of high risk will be the Councils' SIRO, for any other processing will be the designated information risk owner. Processing against DPO advice will be recorded in accordance with ICO guidance.

7. Automated Decision Making

The DUAA allows the Council to use automated systems to make decisions more widely—for example, in service allocation or eligibility checks. Where these decisions have a significant impact, individuals must be told that automation was used and given the chance to challenge it and request a human review.
Automated Decision Making using sensitive data (like health or ethnicity) is still restricted and only allowed with a clear legal basis. Safeguards must be in place to ensure fairness, transparency, and accountability.

8. Accountability and Governance

We will:

- Ensure that processes meet required standards to protect personal data.
- Ensure that sub processors, agents and suppliers meet the same requirement through contract.
- Keep "records of processing activities" (ROPA).
- Conduct DPIAs for high-risk or DUAA-related processes.
- Report data access or reuse activities publicly as required.
- Investigate and respond to any data breaches (this is expanded at Appendix B)
- Keep records of subject request and data breaches for 6 years

Being transparent and providing accessible information to individuals about how we will use their personal data is important to the Council. We will ensure a privacy notice is in place for each circumstance where we are collecting and processing information. (this is further expanded at Appendix C)

9. Security

We will use appropriate **technical and organisational measures**—encryption, access controls, secure storage, contractual clauses and staff training—to adequately protect data. Security controls are contained in the Council's ICT Acceptable Use Policy.

10. Training

Training for all staff includes:

- Induction training.
- Annual refresher sessions.
- Specialist programmes where needed (e.g., SARs, breach response).
- Guidance and training available for members
- Training records will be kept for auditing.

This is expanded at Appendix D.

11. Policy Review

This Policy is reviewed every three years or sooner when significant legal changes occur (for example, DUAA updates).

All updates will be communicated to staff and published as needed.

Data Protection Policy Appendices

Appendix A – Subject Access Requests (SARs)

Appendix B – Data Breach Procedure

Appendix C – Appropriate Policy Document (Special Category & Criminal Data)

Appendix D – Information Sharing & DUAA Compliance

Appendix E – Training & Awareness

Appendix F – Complaints Handling (DUAA Compliance)

Appendix G – Councillors

Appendix A – Subject Access Requests (SARs) and/or rights requests.

Any individual has the legal right to know what personal information the Council holds about them. This is known as a Subject Access Request (SAR). This process applies equally for other rights provided to subjects under UK GDPR.

- A SAR can be made **in writing, by email, or verbally**. Staff should not refuse a request simply because it is not written on a form.
- When receiving a SAR, staff must **check the identity of the requester** before releasing any information. If the request is made by a third party, we must confirm that they have the data subject's written consent or legal authority.
- The Council will apply the DUAA's **"stop the clock"** provision when awaiting clarification from requesters.
- Under DUAA **reasonable and proportionate searches** are required when responding to SAR.
- The Council must provide a response **within one calendar month**. Where the request is complex, the DPO may extend the deadline by a further two months. The requester must be informed in writing of any extension.
- Requests that are **manifestly unfounded or excessive** may be refused, but this decision must be approved by the DPO and explained clearly to the requester.
- If information about other individuals is contained in the records, this data will only be disclosed if it is lawful and fair to do so. Otherwise, it will be redacted.
- If an individual is unhappy with the Council's response, they may make a complaint. Complaints should first be reviewed internally by the SIRO. If unresolved, the individual may escalate the matter to the Information Commissioner's Office (ICO).
- Under the **DUAA**, we are also required to keep a record of requests for access and reuse of public data. This ensures transparency in how public data is made available.
- We will abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DPO about any such request.
- It is essential that you contact the DPO for advice on direct marketing before starting any new direct marketing activity. You must not send direct marketing material to someone electronically (e.g. via email) unless you have an existing business relationship with them in relation to the services being marketed.

Appendix B – Data Breach Procedure

A personal data breach is any event that leads to the loss, destruction, unauthorised disclosure of, or access to, personal information. Examples include sending personal information to the wrong recipient, losing files, or an IT system being hacked.

- Any member of staff who becomes aware of a possible breach must **report it immediately to the DPO**. Staff should not try to investigate or fix the breach themselves without direction.
- The DPO will **log the incident** and carry out an initial risk assessment using the Council's breach risk matrix.

- If the breach is likely to result in a risk to people's rights or freedoms, the Council must **report it to the ICO within 72 hours** of becoming aware of it.
- Where there is a high risk of harm to individuals, the Council will also **notify those affected directly**, explaining what has happened, what data was involved, and what steps they can take to protect themselves.
- Even if a breach does not need to be reported to the ICO, it must still be **logged internally** with details of the cause, impact, and any corrective action taken.
- The Council will review all breaches to learn lessons and improve its systems and training, reducing the risk of recurrence.
- Lessons learnt from data breach incidents will be collated and used to prevent similar occurrences going forward.
- Volumes of data breach, type and impact will be reported to Senior Leadership Team, portfolio holders, and annually in information governance reporting.

Appendix C – Appropriate Policy Document (Special Category & Criminal Data)

The Council often needs to process special category data, such as health information, or criminal conviction data. This is more sensitive than ordinary personal data and requires additional safeguards.

- Special category data will only be processed when **absolutely necessary** and when a lawful condition under Article 9 UK GDPR or the DPA 2018 applies.
- Criminal offence data will only be processed when authorised by law, for example under the Council's safeguarding or enforcement duties.
- The Council will keep a **written record** of the legal condition relied on for processing, the purpose of the processing, and the retention and erasure rules that apply.
- Special category and criminal data will be retained **only as long as necessary** for the purpose for which it was collected and securely deleted once no longer needed.
- Access to such data will be **strictly limited** to staff who need it for their role and who have received appropriate training.
- Under the DUAA, special category and criminal data will **not** be made available for reuse or access unless there is a clear legal basis.

Specifically this policy covers the requirement under Schedule 1 para 39 of the Data Protection Act 2018 for processing dependant on Schedule 1 para 38.

- This includes processing for:
  Health or Social Care purposes (Schedule 1 part 1 section 2) (GP referrals)
- Processing for Public Health. (Schedule 1 part 1 section 3) (Public health England)
- Processing for Research. (Schedule 1 part 1 section 4) (anonymisation of data)

- Processing for Statutory and Government Purposes. (Schedule 2 part 2 section 6) – documented in the Register of Processing Activities.

Appendix D – Information Sharing & DUAA Compliance

The Council shares information with partners and other organisations to deliver services, meet legal duties, and support public safety. Sharing will always be carried out in a controlled and transparent manner.

- No personal data will be shared without a valid legal basis. Before sharing, staff must consult the DPO if there is any doubt.
- Information Sharing Agreements (ISAs) or legally binding contracts will be put in place with external organisations, setting out how data will be used, stored, and protected.
- Any sharing of personal data must be **necessary, proportionate, and secure**. Only the minimum amount of data needed should be disclosed.
- The DUAA introduces additional requirements for **lawful access to public sector datasets**. Where these apply, the Council will ensure data is provided in interoperable formats and with appropriate technical safeguards.
- The Council will maintain a public transparency register of datasets that are shared or made available under the DUAA, showing which organisations have access to the data and for what purpose.
- All data sharing decisions must be logged, and the risks assessed, before any information is released.

Appendix E – Training & Awareness

All staff have a responsibility to understand and follow this Policy.

- Every new starter must complete **mandatory data protection training** as part of their induction.
- All staff must complete **regular refresher training**, with updates provided sooner if laws change (such as new DUAA rules).
- Staff in roles with higher data protection responsibilities (for example, housing, and service managers) will be given additional **specialist training**.
- The Council will keep records of all training attendance. These records will be reviewed regularly to ensure compliance.
- Awareness campaigns, such as posters, newsletters, and intranet articles, will be used to keep staff informed about data protection responsibilities and any changes in the law.

Appendix F – Complaints Handling (DUAA Compliance)

All individuals have the right to raise concerns about how their personal data is handled. The Council is committed to resolving complaints fairly, transparently, and in line with the Data Use and Access Act 2025 (DUAA).

- The Council will provide an **electronic complaints form, and email address** accessible via its website and intranet.
- All complaints will be **acknowledged within 30 calendar days**, with updates provided if resolution takes longer.
- Complaints will be handled **without undue delay**, and outcomes will be clearly communicated to the complainant.
- Where a complaint relates to automated decision-making, data sharing, or reuse under DUAA, the Council will ensure appropriate review and explanation.
- Staff must refer any data-related complaints to the **Information Governance Team** immediately and must not attempt to resolve them independently.
- The **Data Protection Officer (DPO)** will oversee complex or high-risk complaints and ensure lessons are learned.
- The Council will maintain a **complaints log**, including outcomes and corrective actions, for audit and improvement purposes.
- Individuals dissatisfied with the Council's response may escalate their complaint to the **Information Commissioner's Office (ICO)**.

Appendix G – Councillors

Councillors may process personal data in **three distinct roles**, and depending on the context, they may **not be acting on behalf of the public authority** (i.e., the Council). These roles are:

1. **As a Ward Representative**
   When handling casework or assisting residents with personal issues (e.g., complaints, housing matters), councillors act independently. In this role, they are considered data controllers in their own right, not processing data on behalf of the Council.

2. **As a Political Party Representative**
   During election campaigns or party activities, councillors may process personal data under the authority of their political party. Here, the party is the data controller, and the councillor is acting on its behalf—not the Council

3. **As a Member of the Council (e.g., Committee or Cabinet)**
   In this role, councillors are typically processing data on behalf of the Council, which is the data controller. However, if they use data outside of Council purposes (e.g., for personal or political use), they are no longer acting on behalf of the public authority

Understanding these distinctions is crucial for compliance with UK GDPR and the DUAA, especially regarding registration, lawful basis, and data sharing responsibilities