Record Management Policy 2026

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

1. Introduction

This policy establishes the framework for managing records created or received by the authority, ensuring they are accurate, accessible, secure, and retained appropriately.

It supports compliance with various legal and regulatory frameworks.

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

2. Scope

This policy applies to all recorded information held by the authority, regardless of format (paper, digital, email, audio, video), across all departments and services.

This policy applies to the full information or data lifecycle.
This includes:

- the collection or creation of information,
- the storage,
- the use or processing,
- any sharing ,
- any archiving
- and the deletion/destruction of information.

In addition to automated decision outputs, records generated by AI systems must be managed, retained, and reviewed in accordance with this Policy.

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

3. Principles

The Section 46 Code of Practice is official guidance issued under Section 46 of the Freedom of Information Act 2000 (FOIA). It sets out recommended standards for the creation, management, retention, and disposal of records by public authorities in England, Wales, and Northern Ireland. The Code is maintained and updated by The National Archives and is supported by the Information Commissioner's Office (ICO).

In line with the Section 46 Code of Practice, this policy is built on:

- **Accountability** – Records must support transparency and decision-making.
- **Integrity** – Records must be authentic, reliable, and complete.
- **Accessibility** – Records must be retrievable and usable when needed.
- **Security** – Records must be protected from unauthorized access or loss.
- **Retention** – Records must be retained only as long as necessary.

4. Roles and Responsibilities

Each Council is designated "Data Controller" for the data it generates, uses and accesses in delivery of its public task. Clear roles and responsibilities are defined to ensure effective implementation and oversight of this Policy

- **Senior Information Risk Owner (SIRO):** Strategic oversight.
- **Information Governance Team:** Compliance monitoring, advice, liaison.
- **Managers/Service Leads as Information Asset Owners (IAOs)** Accountable for specific datasets
- **All Staff & Members:** Responsible for good recordkeeping practices and compliance with this policy and legislative requirements.

5. Legal and Regulatory Framework

- FOIA 2000 – Section 46 Code of Practice: Sets standards for record creation, retention, and disposal
- Local Government Act 1972: Requires proper custody of records (Section 224)
- Local Government Transparency Code 2015: Mandates publication of key datasets

- Data Protection Act 2018 / UK GDPR: Requires lawful, fair, and secure processing of personal data
- Public Records Act 1958: Governs historical records and transfer to The National Archives.
- Data (use and access) Act 2025: Lawful access to datasets where required, Use of interoperable formats, a transparency register of accessed/shared data.

6. Policy Commitments

As with personal data, all data sharing must be documented and risk assessed by the Information Governance lead. Approval for processing of high risk data will be considered bythe Council's SIRO. fFor any other processing the approval for processing will be considered by the designated information asset owner (IAO).

The Council aims to:

- Maintain a Records Retention Schedule aligned with statutory and operational needs.
- Apply metadata standards to support classification and retrieval.
- The origin and method of creation (e.g., "generated by AI system X on [date]") should be documented to support auditability and public trust where generative AI is used.
- Conduct annual audits to monitor compliance and identify risks.
- Ensure secure disposal of records in accordance with the Section 46 Code.
- Publish required datasets under the Transparency Code.
- Integrate records management into digital transformation initiatives.
- Update and amend a publication scheme.

7. Retention Schedules

Systematically disposing of materials at the end of their life is good business practice and is essential we comply with the law. For each of our activities, the retention schedule sets out:

- What collections of information are held and their purpose.
- Who is responsible for them (the 'information asset owner').
- How long materials need to be kept and what the trigger is to count down to disposal, for example six years from date of case closure.

Whether the retention period is defined in law or based on common business practice. In maintaining our retention schedule, we will:

- Identify the records the Council needs to keep - and those it does not need to retain
- Define how long information is kept to meet the legal, financial and other requirements of public administration.
- Apply those rules systematically to its information.
- Confirm how information will be stored at different stages of its life-cycle and how it will be destroyed at the end of its life.
- Provide evidence that records have been disposed of consistently in case of challenge.
- Mark and include AI-generated records in the "Retention Schedule" and dispose of them in accordance with statutory and operational requirements.

9. Security

We 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 by the relevant manager on record management arrangements.
- Guidance available to all staff.
- Specialist programmes where needed (e.g., Information asset owners).
- Training records will be kept for auditing.

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.