CITY OF WOLVERHAMPTON COUNCIL

Records Management Policy

1. Introduction

City of Wolverhampton Council (the Council) recognises that records are valuable assets and vital to the delivery of high quality public services. Effective records management is essential in enabling the Council to comply with its legal and regulatory obligations.

The Council is committed to establishing and maintaining recordkeeping practices which provide evidence of its activities, demonstrate transparency, provide reliable information for its stakeholders and safeguard all personal data held. For the avoidance of doubt, the following definitions will apply:

- **Records** are information, received and maintained as evidence;
- **Information** is knowledge that has been recorded;
- **Documents** are items created in council systems. Some may be records, some may not be.

2. Purpose

2.1 The purpose of this policy is:

- To ensure council activities are documented to meet business needs, accountability and legal requirements through effective recordkeeping practices for creating, controlling, retaining and disposing of records.
- To ensure the integrity and authenticity of records to allow well-informed decision making by the Council
- To acknowledge the importance of effective records management and demonstrate the Council’s commitment to this.
- To act as a mandate for effective recordkeeping practices across all of its activities.
- To make employees and third parties aware of their recordkeeping responsibilities.
- To set out the Council's corporate approach to records management, in accordance with British Standard and International Standard (BS/ISO) 15489-Records Management, and as required under the Lord Chancellors Code of

Practice on Records Management, issued under Section 46 of the Freedom of Information Act 2000.

- To support the Council's responsibilities as Data Controller under the Data Protection Act 1998, Data Protection Bill 2017 (which updates data protection laws for the digital age), and the General Data Protection Regulation 2016/679 (GDPR). Also, as a public authority subject to the Freedom of Information Act and related legislation.

3. Scope

3.1 This policy applies to all permanent and temporary employees of the Council and also applies to those acting as agents, contractors or consultants and councillors acting on behalf of the Council in the course of carrying out its functions.

3.2 It applies to all records regardless of their format. A record is recorded information, in any form, which is created or received by the Council and maintained as evidence of its activities and transactions. Records can include any of the following:

- Paper documents
- Scanned documents
- Electronic documents including Word documents, spreadsheets and presentations
- Emails which document business activity and decisions
- Audio and video tapes, cassettes, CD ROM etc
- Text messages
- Minutes of meetings
- Microfiche/film
- Plans, drawings and maps
- Case notes and updates
- Notes of telephone and Skype conversations

3.3 Records management is the process used to manage records at each stage of their lifecycle. From creation, when naming conventions, version control and metadata[1] are applied, through active use when records need to be tracked and safeguarded from unauthorised access, to retention, when they need to be safely and securely stored for as long as they’re needed for business and legal purposes, to appraisal and disposal in line with retention and disposal criteria.

4. Roles and responsibilities

[1] A very general term for metadata is “data about data”. Examples of metadata include title, subject, date created and creator.

4.1 Everyone who is employed by the Council (permanent and temporary members of staff, agents, contractors and consultants) has a responsibility to create records that document their official activities and manage them in accordance with the Council's policies, standards, procedures and guidelines.

4.2 Records created and received in the course of council business activities form part of the corporate memory and do not belong to the employee, agent or contractor who created or received them. They must therefore be preserved and safeguarded for as long as they're needed for business and legal purposes in the appropriate recordkeeping system where they can be shared with whoever has authorisation to access them. This applies to all records regardless of their physical location or format.

4.3 Records must be reliable and contain full, accurate and up to date information. They should be created at the time of the business activity to which they relate, or as soon as possible after it. The creation of appropriate records should be incorporated into local business processes based on business needs, regulations and stakeholder expectations.

4.4 Records must be usable and located in official recordkeeping systems where they can be preserved until the end of their retention period and easily retrieved. Their content and context must be understandable to whoever has authorisation to access them. It should be clear as to why the record has been created, who created it and when it was created. Records relating to the same business activity should be grouped together and cross referenced regardless of their format. Employees must ensure conformance with any titling and classification instructions for their business area at the time the record is created or captured in the official recordkeeping system.

4.5 Official records should not be held in personal drives or Outlook email boxes as these do not have adequate record keeping functionality and cannot ensure access and evidence of business activity over time.

4.6 Records will rarely need to be duplicated and personal copies of records should not be created and kept. Any ephemeral information (non-records) should be disposed of immediately after it is no longer required.

4.7 Records must be trustworthy and should therefore be safeguarded against alteration and damage. Any authorised amendments must be clearly identified and traceable. The Council's policy is to create, store and manage its records electronically. Electronic records not held to an acceptable standard will lose much of their evidential value. It is important therefore that the scanning of records should comply with British Standard, BS10008 and any migration of records from one system to another be carefully controlled.

4.8 Records must be kept secure from unauthorised access according to the sensitivity of their content and the correct protective marking procedures followed. All employees must have completed the mandatory protecting information training and apply this to all handling of records, including when transporting records and when remote working.

4.9 The Council's records must be held only as long as they are needed to meet business, legal and regulatory requirements. They should then be disposed of in line with Retention and Disposal Schedules and the Confidential Information Disposal Policy referred to in paragraph 6. Retention and Disposal Schedules should be maintained and implemented by service area managers with guidance and advice provided by the Records Manager. Any records which contain, or may contain, content relating directly or indirectly to the sexual abuse of children must be retained as they fall under the terms of reference of the Independent Inquiry into Child Sexual Abuse (IICSA). Any records deemed worthy of historical interest must be notified to the Records Manager who will arrange for their transfer to the City Archives for preservation.

4.10 Clauses on record keeping responsibilities must be included in contracts with third parties and partner organisations. It must be made clear from the outset the standard of record keeping expected and where responsibility for holding the records will rest. If appropriate, records management training and guidance will be provided for the partner organisation.

4.11 Directors and managers are responsible for ensuring they manage the records relating to their business areas in accordance with records management policy and procedures. They must ensure any new employees or contractors are made aware of the policy and undertake relevant information and records management training. They must ensure any potential risks to compliance are identified, assessed, recorded and appropriately mitigated and managed.

4.12 The Records Manager is responsible for providing advice and ensuring records management policies and procedures are established in line with legal requirements and professional best practice standards.

4.13 Staff at the City Archives have responsibility for preserving some records which need to be kept in the long term including historical records deemed worthy of permanent preservation.

4.14 Social Care Caldicott Guardians are responsible for ensuring that personal identifiable information is protected and shared appropriately.

4.15 The Senior Information Risk Owner (SIRO) chairs the Information Governance Board and has overall responsibility for managing information risk. Information Governance issues are reported to the Board by the Information Governance Team and progress on records management is reported on a regular basis by the Records Manager.

4.16 The Information and Communication Technology (ICT) Team is responsible for data storage, backup and disaster recovery for in-house systems which hold the Council's electronic records.

4.17 The Resilience Manager is responsible for coordinating business continuity planning and working with service managers and the Records Manager to identify and safeguard priority business areas, systems and vital records.

4.18 The Strategic Executive Board and Managing Director have overall responsibility for ensuring appropriate resources are in place.

5. Risks

5.1 The Council recognises that there are risks associated with non-compliance with the law. This policy aims to mitigate risks such as:

i) Significant risk to the Council, its customers, partners and stakeholders;
ii) Inappropriate disclosure of information, leading to major incidents;
iii) Legislative or financial penalties;
iv) Loss of reputation and damage to the Council's corporate image.

6. Relevant legal requirements and standards:

- Local Government (Records) Act 1962
- Local Government Act 1972
- Freedom of Information Act
- Environmental Information Regulations
- Data Protection Act 1998
- Data Protection Bill 2017
- General Data Protection Regulation 2016/679 (GDPR)
- Human Rights Act
- Legislation specific to service areas
- The Independent Inquiry into Child Sexual Abuse (IICSA),
- BS10008 Evidential weight and legal admissibility of electronic information
- National Archives Guidance
- The Lord Chancellor's Code of Practice Under Section 46 of the Freedom of Information Act 2000
- BS ISO 15489-1:2001. Information and documentation. Records Management

7. Related policies:

- Confidential Information Disposal Policy
- Data Protection Policy
- Freedom of Information Policy
- Information Governance Policy
- Information Incident Policy
- Information Protective Marking & Handling Policy
- Information Risk Policy

- Information Security Policy
- Information Transparency Policy

8. Compliance and monitoring

7.1 Compliance with this policy will be monitored by the Records Manager and regular reports on progress will be submitted to the Information Governance Board. It will be reviewed annually to ensure it is up to date.

Change History

Version	Date	Description	Author	Role
2.1	14/12/15	Revised policy replaces Records Management Policy 2.0 published 18/12/12	Catrina Finch	Records Manager
2.2	13/01/16	Incorporation of amendments from the Information Governance Board	Catrina Finch	Records Manager
2.3	18/01/16	Incorporation of some further amendments from Information Governance	Catrina Finch	Records Manager
3.0	21/01/16	Final version	Catrina Finch	Records Manager
4.0	16/03/18	Revised following legislative changes	Catrina Finch	Records Manager

Approvals

Information Governance Board	18/01/2016
Strategic Executive Board	09/02/2016
Information Governance Board	22/03/2018

Publication

Policy Portal	February 2016