Records Management Policy

Author: Rachel Everitt

Date: January 2025

Version: v0.1

Title	Records Management Policy
Author	**Rachel Everitt**
Owner	**Data Protection Officer**
Created	**January 2025**
Approved by	**Audit Committee**
Date of Approval	**February 2025**
Review Date	**February 2027**

Document Version Control

Document Version Control	
Issue Number	Date
0.01	January 2025

This is a live document effective from the issue date. It supersedes any previous versions of this document, which are now withdrawn.

Contents

1. Introduction

Bury Council recognises that records are valuable assets and vital to delivering efficient, high quality and value for money public services. Managing records effectively is essential in enabling the Council to comply with its legal and regulatory obligations in protecting the right of the Council, its employees and the residents of the borough.

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

This policy is part of Bury Council's Information Governance Framework and should be read in conjunction with the other policies and procedures within the framework.

Scope

This policy applies to all records created, received and maintained by all officers, temporary staff, consultants, contractors, elected members and others in the course of their work for and on behalf of Bury Council, whether working directly for the Council or in partnership with it.

The policy applies regardless of location of working environment, that is, council premises, at home or elsewhere.

2. Definition of Records

Records are defined as information that is created or received, captured, and maintained as evidence of the business of the council, due to its operational, legal, financial, or historical value to the organisation.

This policy covers records in all physical and electronic formats, including, but not restricted to:

- Paper
- Scanned documents/images
- Electronic documents
- Emails
- Notes of telephone conversation or meetings
- Voicemail
- Microsoft Teams, including chats, channels and files
- Web records such as blogs, wikis and discussion threads
- Social media used for business purposes, such as Twitter
- Messaging apps including WhatsApp when used for business related activities
- Visual images such as photographs
- Microform, including microfiches and microfilm
- Records stored on removable media, such as audio and video tapes, memory sticks,
- CDs, DVDs and cassettes
- Published web content (Intranet and Internet)
- Databases and spread sheets
- CCTV

This policy does not cover documents that are not council records, for example non-work related emails, stationery or reference material.

Records created by elected members in their capacity as representatives of the council are covered by this policy. If elected members create records when acting on behalf of their constituents or as a representative of a political party, it is not expected that they personally manage these records in accordance with this policy.

Records

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/electronic location or format.

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 processes based on business needs, legislation, regulations, and stakeholder expectations.

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.

Storage of records

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

Records must be moved from these into the official record keeping system appropriate to each service area. Records will rarely need to be duplicated and personal copies of records should not be created and kept.

Protection of records

Records must be trustworthy and should therefore must not be altered or damaged in any way. Any authorised amendments must be clearly identified and traceable and a copy of amendments kept as an audit trail. The Council's policy is to create, store and manage its records electronically where possible.

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.

Unauthorised access

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.

Retention of records

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 securely in line with Retention and Disposal Schedules.

Retention and Disposal Schedules should be maintained and implemented by managers with guidance and advice provided by the Information Governance Team where required.

Any records deemed worthy of historical interest must be transferred to the Archives team for preservation.

Agile working

All employees, whilst mobile working or working from home, must remain aware of the sensitivity of the information they are handling and ensure it cannot be seen or overheard.

Laptops should be locked when not in use, even for short periods, and password security maintained. Records should be accessed electronically via official council systems and paper records should not be transported off site, unless this is unavoidable. If paper records do have to be taken off site, they must be kept securely at all times to ensure against unauthorised access, loss or damage.

Disposal of records and IT equipment

Personal or confidential information that has reached the end of its retention period and is no longer needed must be securely disposed of. The Council has a contract for the secure disposal of paper records and any confidential paper waste should be disposed of using the confidential waste bins located in council premises.

Any IT equipment, or electronic storage media, which needs to be disposed of must be returned to IT Services for secure disposal.

Responsibilities of 3rd party contractors

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.

Records Management Good Practice

Good records management practice relies on the following:

- Determining which records should be created or received and retained
- Determining corporate record systems for the storage and management of records
- Creation or receipt of required records and their capture into corporate record systems together with related metadata
- Appropriate maintenance of records in safe secure environment(s)

- Determining why and how long records should be kept and how they should be disposed
- Retaining records only for as long as they are needed to satisfy legal, regulatory requirements and operational needs
- Routine, timely and secure disposal of records in line with the Council's retention and disposal policies
- Routine disposal of temporary documents and information (non-records)
- Ensuring data sharing agreements are in place where council records are shared (where there is a legal basis to share) with the public, partners, or contractors, and that this is done in a lawful and secure manner.

3. Compliance and Monitoring

Legal and professional Obligations

Bury Council will take actions to comply with the relevant legal and professional obligations.

Training

Bury Council will provide relevant training both online and face to face to ensure that staff understand the legislation and its application to their role.

All staff must complete mandatory training every year and undertake any further training provided by Bury Council to enable them to perform their duties appropriately.

Completion of training will be monitored by the Policy and Compliance Team and all employees must have regard to the Data Protection Legislation and this policy when collecting, accessing, using, disclosing or destroying personal information. Failure to do so may result in disciplinary action and legal prosecution.

If an employee is in any doubt about how to handle personal or special category data they should speak to their line manager or contact the Policy and Compliance Team by emailing IG@bury.gov.uk.

Policy review

This policy will be reviewed regularly by the Policy and Compliance Team to ensure that it is updated in line with any change in legislation.

Bury Council will continue to review the effectiveness of this policy to ensure that it is achieving it intended purpose.

Any breaches of the principles in this policy must be reported to the Policy and Compliance Team immediately at ig@bury.gov.uk.

Where staff fail to follow and comply with this policy it may result in disciplinary action via the HR channels