POL011

Records Management Policy

Policy Review Date	March 2020

Contents

1 Introduction

Information is at the centre of everything Blackburn with Darwen Borough Council does.

By reading this policy document you will understand the importance of records management; the risks of failing to adhere to the policy and how to implement the values.

2 What is a Record?

Records form part of the corporate memory of the Council and are a valuable corporate resource. Responsibility for the capture and maintenance of records rests with everyone in the Council, all staff should ensure that they are familiar with the policy and comply with the retention policy and schedule.

All records are information assets and hold value.

The Council has a duty to manage records effectively in order to control costs and ensure that information is accessible, authentic, and accurate.

Records capture business activities and transactions, such as contract negotiations, business correspondence, personnel files, and financial statements, just to name a few.

Records come in many formats, including:

- Emails and attachments
- Paper – Memos, Reports, Marketing Materials
- Databases and Document Management Systems
- Servers and Shared Drives
- Website
- Memory Sticks
- CD Rom

Records Management is vital to effective service delivery.

3 Data Retention

3.1 Why do we need a retention schedule

Effective records management procedures are essential if the Council is to meet its legislative responsibilities and protect its vital records.

Vital records are necessary to recreate the legal and financial position of the organisation, preserve the rights of the organisation, its employees and others associated with the organisation.

Legislative responsibilities include compliance with Acts such as the General Data Protection Regulation 2016, Data Protection Act 2018, Freedom of Information Act 2000 and the Local Government Act 1972.

The policy and schedule also need to take account of specialist guidance (issued by bodies such as the Information Commissioner's Office) and professional codes of practice, including specific guidance in relation to inquiries such as The Goddard Inquiry, where we may be instructed to keep records for longer than their specified retention period.

Services User's and the general public will be advised of the retention for specific data sets within the service specific privacy notices held within the Councils Privacy Policy.

3.2 What does the Retention Schedule Cover

The Retention and Disposal Schedule is an essential component of an efficient and effective records management system. The schedule details the retention periods for records and the policy contains guidance on records management to ensure:

- We identify records that we want to keep permanently as part of the local archives;
- The prevention of the premature destruction of records that need to be retained for a specified period to satisfy legal, financial and other requirements of public administration
- Consistency when destroying records not required permanently
- Provision of records management policies to promote good practice in line with ISO15489-1:2016 International Records Management Standard.

4 Risk Assessment

Risks have been assessed as follows:

- Loss of vital records could result in disruption to the Council's critical services
- Inadequately kept records could result in lost income, especially grant income or VAT
- Poorly managed documents could leave the Council vulnerable to loss through theft, duplicate payments or other poor practices and would contribute to a weakening of the system of internal control
- Unnecessary exposure to information loss, such as loss of equipment or manual data, theft or inappropriate sharing of data which constitute a breach of the current UK Data Protection legislation
- Poorly managed document systems make retrieval of information resource intensive
- Inadequate records could result in the Council being unable to defend or pursue legal claims

Departments must ensure that they assess the risks (eg business continuity) involved in the possible loss of records as a result of serious incidents occurring (fire/flood etc.).

A record of the risks and controls should be kept in the departmental risk registers.

5 Quality of Records

This document covers the storage, management, version controls, weeding and archiving of council records both electronic and paper. It is expected that the content of records kept will be of a high quality. The responsibility for the quality of records lies with the Information Asset Owner producing them.

6 Grant Funded Regimes

All staff should be aware that certain grant funding regimes require some documents to be kept for longer than is held in this policy. If that is the case records and documents should be held for the LONGEST period, this will enable both regimes to be complied with.

7 How can I manage records effectively?

We all use records and information on a daily basis to achieve objectives. It is critical that we have the right information in the right place, at the right time, in order to:

- Perform daily business transactions
- Deliver goods and services consistently
- Comply with legislative and regulatory requirements
- Manage risk
- Account for past decisions
- Plan future projects
- Protect the interests of all customers inside and outside of the Council
- Provide documentation of research for the development of products and services
- Enable promotion and publicity, communications, and other reporting
- Preserve the organisational identity and history

Good records management is defined as the systematic control of records throughout their life cycle and involves:

- Creating accurate and complete records to convey information;
- Using records appropriately and storing them securely;
- Retaining records in line with legislative or business requirements once they are no longer active pieces of work;
- Accessing records when needed by ensuring they are easy to locate;
- Disposing of records carefully and securely. Some records have permanent or archival value whilst others can be destroyed when their retention period expires.

7.1 How does it affect me as an employee?

Failure to manage and protect records could have a significant effect on the efficient operation of the Council

Poor records management may also cause the Council to be in breach of its obligations, resulting in security breaches, legal undertakings, and fines.

Each employee has an important role to play in protecting information by managing records in accordance with the Council's established policies and procedures.

This Policy includes guidance to assist you in the following areas;

- Appendix A – Version Control Guidelines
- Appendix B – Weeding or File Stripping Guidelines
- Appendix C – Data Destruction Guidelines
- Appendix D – Transfer of Records to Archival Storage Guidelines
- Appendix E – Standard Operating Procedure

It is important that all staff are familiar with the guidance provided and that you know who to contact in the event of any queries.

8 Compliance

This policy has been adopted by the Council to meet local needs while providing a consistent approach to record keeping. We should also ensure that policies belonging to third party data processors for retaining records are in line with our retention guidance.

To ensure legislative compliance:

- Service areas must be specific and transparent about how long they retain data
- Records must be destroyed in accordance with the retention schedule
- Justification should be provided for records kept longer that the specified period in the retention schedule
- Backup copies and test data stored on alternative media should be destroyed in accordance with the retention schedule
- Records for permanent preservation should be archived securely in a safe location.

9 Review of Records Management Policy

The Information Governance Team will review the Records Management Policy and the Retention and Disposal Schedule as and when they are made aware of amendments to retention guidelines – for example due to changes in legislation or working practices.

Departmental Information Asset Owners (IAOs) are responsible for ensuring changes to structures or working practices within their department are notified to Information Governance.

Associated risks to changes in legislation will be reported to the Senior Information Risk Officer and also to the Chief Executive and members through the Management Accountabilities Framework and the Risk Assessment System.

Directors have responsibility for ensuring compliance with the assistance of the trained members of the Information Governance Section. Compliance will be monitored by the Senior Information Risk Officer (SIRO).

10 Scope

This document applies to all Councillors, Committees, Departments, Partners, and Employees of the Council, contractual third parties and agents of the Council who process, have access to, or custody of, Blackburn with Darwen Council records.

All users **must** understand and adopt use of this policy.

APPENDIX A: Version Control Guidelines

The first prepared/saved document is to be given version 0.01 this indicates it is in draft format.

An accepted version would be issued with the following mark 1.0 this indicates the version is no longer a draft document.

Any minor release update following on from this would be 1.01, thus the first number after the decimal is reserved for release of draft versions or updates.

This enables staff to be aware of the latest version of a document and for logical electronic searching.

For example, the following represents a typical document standard of version control:

Version Control Standards 0.01	(draft)
Version Control Standards 0.02	(still draft)
Version Control Standards 1.0	(accepted version – i.e. put to its designed use)
Version Control Standards 1.01	(an update draft of version 1.0, not yet released)
Version Control Standards 1.02	(still an update draft, not yet released)
Version Control Standards 1.1	(a minor update in final format released for use)
Version Control Standards 1.11	(a draft update to version 1.1)
Version Control Standards 2.0	(a major update i.e. a review - final version released)

This standard should also include a document control form for each version (if required, template attached) which would map the main changes to the document and why the change has caused a version change.

Document control form.

In conjunction with the Councils Records Management Policy and the above Version Control Guidelines section, please see suggested document control form;

Document title *(Include document type in Title e.g. Policy, Strategy, Procedure, Guidance)*	
Version number *(If the document is new start with v0.01)*	
Author of document *(Person + Job Title, and or Committee/group)*	
Authorised date *(when agreed at committee or group)*	
Authorising authority *(name of committee or group or person)*	
Document review date *(date you intend to review and/or revise)*	
Document Distribution *(intended audience)*	

APPENDIX B: Weeding or File Stripping Guidelines

At different times, all data outlives its life and becomes incorrect. At this point we need to delete this data. Disposal is also known as “weeding” or “file stripping”.

It is recognised that the Council currently holds a considerable amount of records, much of which is very old and it is likely that it is overdue for review. It is suggested that planned days be put aside for a review and the possible destruction of old paper files and computer data. Once the backlog has been cleared this policy should followed to ensure that retention of records is controlled.

The Authority and its departments must be able to identify the parts of information held in its records that are a permanent part of the record and those transitory parts that can therefore be discarded. This involves retaining some records, partial disposal of other records and complete disposal of others

The Weeding Process

Departments must consider the following when weeding/file stripping data:

- Departments must set aside a reasonable period to review their files. This will depend on the size of files, the frequency with which data changes, and legislative requirements. A record of reviews undertaken should be evidenced, for example by using a ‘review’ sheet to record reviews and the potential destruction date.

- Departments must refer to the Council’s Retention and Disposal Policy and Schedule considering what can be deleted, and when. They must also ensure that all their record-types are listed in the retention schedule, to ensure consistency of use and Records management practice.

- Departments must keep an index system for manual, usually paper, records. It is vital to ensure that the index is kept up to date, or it will soon become out of date, and will lead to mistakes being made.

- For electronic file lists, for example computer files, Departments must be able to add disposal and review dates to file entries, and run a yearly (or quarterly) search for all records that have disposal/review dates that have already passed. Departments must adopt electronic records management applications that can undertake this task with regard to electronic records, setting disposal dates for record types as appropriate.

- Departments must list all files sent for archive storage to enable future access. In Addition an index should be maintained of the paper files in that department.

APPENDIX C: Data Destruction Guidelines

Where, after due consideration, it has been decided to permanently destroy data that is no longer required, then the following general principles should be applied:

- Items containing personal and/or sensitive data should only ever be disposed of in confidential waste bins.
  Note: Personal data is any data from which an individual can be identified.
  Sensitive or Special Category data includes racial, ethnic, political, religious or philosophical beliefs, trade union memberships, genetic biometric or health data, or data concerning a person's sex life or sexual orientation.

- All other items should be disposed of in standard green recycle disposal bins. If unsure please contact the Data Protection Officer for guidance

- To permanently clean or delete data from reusable media including computer hard discs, CDs, DVDs and memory pens, the use of a reliable 'electronic shredding' tool should be employed wherever possible, or check with ITM&G

- Where a computer has become unserviceable and is to be replaced or discarded but may still contain sensitive data on its hard disk, ITM&G support engineer will remove the hard disc unit from the computer prior to the equipment's disposal

- Where the affected hard disk is confirmed as unserviceable and is to be discarded then it should be made permanently unusable by physical destruction

- Where non re-writable archive media is to be discarded, then it should be disposed of in a way that makes it unusable. For example, CD-ROMS may be heavily scratched on their recorded face with an abrasive material and the disk then broken into parts. Please note here that care must be taken to avoid personal injury

- The use of incineration facilities and commercial contractors providing specialist disposal services may also be considered as appropriate, subject to appropriate contracts being in place

APPENDIX D: Transfer of Records to Archival Storage

The Council has an existing process that manages off-site archiving of hardy copy documentation. This process includes archiving, storage, recall and destruction in-line with pre-agreed destruction dates.

Anyone wishing to transfer permanent records to archival storage should contact the CAPS team who manage the archive function.

APPENDIX E: Standard Operating Procedure (SOP)

Some records do not need to be kept at all. This document defines types of records that may be routinely destroyed in the course of business.

This SOP usually applies to information that is duplicated, unimportant or only of short-term value. It includes:

- 'With compliments' slips
- Catalogues and trade journals
- Telephone message slips
- Non-acceptance of invitations
- Electronic mail messages or notes that are not related to authority business
- Requests for stock information such as maps, plans or advertising material
- Out-of-date distribution lists
- Working papers that lead to a final report

Duplicated and superseded material such as stationery, manuals, drafts, forms, address books and reference copies of annual reports must be destroyed under SOP.

These guidance notes cover both electronic and hard copy records. Special care should be paid to ensuring that electronic systems can adequately meet requirements for:

Deleting electronic records, especially those held on archive or long term back-up media
Recovering electronic records from archive or long-term back-up media, regardless of changes to technology that may have occurred since the records were saved.

SOP **DO NOT** relate to records or information that can be used as evidence i.e. to prove that something happened. If you are in doubt about what information is required consult with the Data Protection Officer.