RECORD MANAGEMENT AND RETENTION POLICY

Name of Author	[redacted]
Department	Information Governance
Owner	Head of Information Governance
Authoriser	Strategic Director Resident Services, Senior Information Risk Owner (SIRO)
Published Date	
Version	3.0
Copies To	
Classification	Internal Use Only

Revision History

Version	Date	Revision Author	Summary of Changes
1.0	January 12, 2016		
2.0	August 24, 2018	[redacted]	
3.0	Nov 10, 2020	[redacted]	Updated roles and responsibilities

Distribution

Name	Position	Date circulated
[redacted]	Head of Information Governance and DPO	August 24, 2018
[redacted]	Head of Information Governance and DPO	December 14, 2020
Information Risk Board	SIRO, Information Asset Owners and Deputy Information Asset Owners	November 2, 2021

Approval

Name	Position	Date of sign off
[redacted]	Senior Information Risk Owner (SIRO), Strategic Director Corporate Resources	October 5, 2018
[redacted]	Strategic Director Residents Services, Serious Information Risk Officer (SIRO)	November 30, 2021

Contents **Page**

1. INTRODUCTION

The definition of Records Management is the management of all documents and records (in all technical or physical formats or media) of an organisation throughout their lifecycle, from the time they are created to their eventual disposal. A Record is an account of facts, events or transactions that needs to be preserved. A Record generally comprises of a number of datasets that provide facts and analysis for future reference.

Record Retention is an aspect of Records Management that defines the time period records should be maintained prior to disposal or long-term archiving. Legal considerations, service delivery needs, safe storage, and on-going access requirements all influence records retention.

The purpose of this policy is to outline how the Council's requirements for records management and retention should be undertaken. Records are a key information asset for the Council and should be managed to enable the organisation to:

- Deliver quality services by having timely access to meaningful and appropriate records.
- Make informed decisions based on reliable recorded data.
- Protect vital records for future reference.
- Drive information security through excellent records management.
- Drive an open data culture and make records available as appropriate to support transparency.
- Respond appropriately to record data subject requests from the public.
- Comply with the law.

1.1 Definitions

'Archive records' are those records which need to be held indefinitely for reference or legal purposes, or because their historical value.

'Current records' are those records that are in regular use and needed for the conduct of current business.

'Semi current records' are those records which are no longer needed for the conduct of current business, but still need to be kept for a defined period for reference or audit/legal purposes and may have potential for permanent preservation because of their historical value.

'Structured records' are those records held within a database, application (Inc. email) or filing structure that enable their easy retrieval.

'Vital records' are those records whose long term preservation must be ensured to allow the Council's functions to continue. These records are usually those which cannot easily be

reproduced, if at all, from other sources and as such create an increased risk impact for the Council, as identified in divisional business continuity plans.

"Information user" refers to all staff, elected members, contractors, agents and representatives and temporary staff working for or on behalf of the Council who have access to Council records, whether paper, electronic or audio-visual (including emails produced or received in the conduct of business; It also includes records managed on behalf of the Council by an external body such as a contractor).

1.2 Key Roles and Responsibilities

All staff at Lambeth Council who create, have access to, maintain, or contribute to Records have a prime responsibility for day-to-day record management, as do their line managers.

Anyone creating, receiving, accessing, storing, or disposing of records on behalf of the Council must be made aware of their record keeping and information management responsibilities through the appropriate provision of training and the issuing of guidance.

Training and relevant communications will be provided to ensure that staff are aware of their obligations regarding Data Protection, Freedom of Information, and information management.

More detailed training will be provided for specific groups of staff whose duties mean that they handle large amounts of sensitive data on a daily basis.

Each individual is responsible for ensuring that they receive this training and that they have read and understood the relevant policies and guidance. All staff need to ensure that records are managed in accordance with the record management lifecycle.

Any record management issues must be resolved promptly and accurately and be reported if appropriate and communicated to the Deputy Information Asset Owner, Data Owner or Information Asset Owner. Employees, agents and contractors leaving the Council must take appropriate steps to ensure that records that they have been handling or storing as part of their role continue to be accessible after they have left the Council.

The line manager of the individual leaving the Council must make arrangements with leavers to ensure that such records continue to be available to protect the Council's corporate knowledge.

These arrangements should include the identification, return and collation of records held locally or within the email account of the leaver.

Key Roles

There are a number of senior roles within Lambeth Council that have key responsibilities within the Records Management and Retention Policy.

The Enterprise Architect

The Enterprise Architect is responsible for designing the Council's **information architecture,** including its logical and physical data assets and data management resources.

The Enterprise Architect will work with key stakeholders both internal and external to ICT (directors, service managers, business liaison managers and subject matter experts) to build a holistic view of the Lambeth Council's strategy, processes, information, and information technology assets.

The role of the Enterprise Architect is to take this knowledge and ensure that the business and ICT are aligned. Record Management is a key consideration in planning the data architecture and ensuring systems can create the underlying technology and information architecture to support the records management lifecycle, in particular in terms of ease of access and maintenance, auditing, retention and disposal.

Directors and Heads of Service

Directors and Heads of Service are responsible for considering Information Governance implications when planning to out-source services, work with partners or commission new technologies or major structural changes. Records Management considerations must be specified at the outset with suppliers and partners and built into service and technology specifications.

The Caldicott Guardian

The Caldicott Guardian position is held by the Director of Public Health, who is the senior person responsible for protecting the confidentiality of individuals using care and support services and enabling appropriate information sharing.

Good record management practice is a key consideration for the Caldicott Guardian in discharging their responsibilities. The Caldicott Guardian is the person with overall responsibility for protecting the confidentiality of personal data across Lambeth Council.

The Caldicott Guardian plays a key role in ensuring that Lambeth Council and partner organisations abide by the highest level for good record keeping standards for handling personal data.

The Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) role is currently held by the Strategic Director, Corporate Resources. The role:

- Is accountable for information risk management.
- Fosters a culture for protecting and using data.
- Provides a focal point for managing information risk and incidents.
- Is concerned with the management of all information assets.

The SIRO has overall accountability for the risk management requirements outlined in this policy and will oversee Records Management with specific interest in the reliability and protection of data in line with the Data Protection Act 2018.

Information Asset Owners (IAO)

IAOs are strategic directors leading each directorate. Their role is to understand what information is held within their business area, what is added and what is removed, how information is moved, who has access and why.

They will ensure adequate records are in place which document their areas activities. IAOs shall establish, maintain and update the Information Asset Register (IAR) and retention periods for the personal data processed by their service area(s).

The quality of record management to support the maintenance of information assets is a key responsibility of an IAO. The IAO will be responsible for ensuring that record management is incorporated into all relevant operational procedures and that these procedures are properly implemented and monitored regularly.

Deputy Information Asset Owners (DIAO)

DIAOs are assigned to support IAOs in coordinating compliance with the Information Governance Framework and act as first point of contact for local managers and staff seeking advice on records management and the application of retention schedules. The DIAOs ensure information handling procedures are proportionate to the risk and are applied across their division.

In collaboration with the IAO, the DIAO ensures that information is securely destroyed in line with the Lambeth Retention Schedule, reporting any issues or concerns over data quality held within their division.

The DIAO is responsible for compliance of data processing and data sharing agreements ensuring that information stored, managed or hosted elsewhere is maintained and managed in line with contractual arrangements.

Data Owners (DO)

The DO ensures that information assets held by their service area are accurate and up to date at all times, holding day to day responsibility for record management practice for the information assets under their ownership. DOs are responsible for ensuring that this policy is fully operational and understood by staff in their operational area.

It is the responsibility of the DO to reflect the unique characteristics of their information assets onto the information asset register ensuring that this record is complete and accurate at all times. In addition, the DO monitors user access to information assets to protect from unauthorised access or misuse of data.

Data Protection Officer (DPO)

The DPO is the Head of Information Governance and is responsible for ensuring the organisation meets its statutory and corporate responsibilities and engenders trust from the public in the management of their personal information. The DPO is accountable for overseeing monitoring and spot check processes in relation to all policies and reporting to the Senior Information Risk Owner on compliance with the Council's policies.

Information Security Officer

The Information Security Officer is responsible for providing information security advice to the Council. Information security has a key role in supporting good record management practice, ensuring that records cannot be corrupted or changed without agreed access and permissions. Any security issues impacting on the integrity of records will be reported to the relevant IAO for resolution.

2. POLICY REQUIREMENTS

This policy will act as a single reference point for the principles that will govern Records Management:

2.1 Records Management Overview

Adequate records must be created, maintained and kept secure to meet the Council's business needs and to account fully and transparently for all actions taken and decisions made. Such records should:

- Provide credible and authoritative evidence.
- Protect legal and other rights of the Council, its staff and those who have dealings with the Council.
- Facilitate audit.
- Fulfil the Council's statutory obligations.

Records must be created, wherever possible, in an electronic format to support the Council's commitment to be digital by default and reduce physical storage issues. Records should be configured to support information sharing and enable neutral location working as appropriate.

Records should be complete, accurate and up to date, and the data and information they contain should be reliable, with evidence available to demonstrate authenticity.

Records should be efficiently identified and retrieved by those with a legitimate right of access, in line with the Council's policies and applicable statutory requirements, for as long as they are held by the Council and its agents, irrespective of any changes in physical or electronic format.

Records should be kept secure from unauthorised access, alteration, reproduction or destruction, and access and disclosure properly controlled and documented (in line with the Council's policies and procedures).

Vital records, which the Council must have in order to carry out its legal responsibilities in an effective manner, must be properly protected to ensure continued accessibility.

Consistent and documented retention, appraisal and disposal procedures must be in place to ensure that records are securely destroyed when no longer required, or passed to archives or offsite storage for continued retention or permanent preservation. Records that are passed to archive for preservation, or offsite storage, should be appropriately logged/indexed to enable retrieval should this be required.

Steps must be taken to enable the continued access to electronic records and records held in other forms that are subject to lengthy retention periods or which are required for permanent preservation. Appropriate procedures will be put into place to ensure that the continued access to these records is maintained for as long as is required.

Digital records must comply with the Digital Continuity Policy to avoid information loss and also to ensure that records are not retained inappropriately.

Intellectual property rights relating to records and information will be respected, where appropriate reuse of records and information by third parties will be permitted in support of legitimate aim(s) of the Council or its partners.

Records and information will be processed in accordance with the Council's Information Protection and Handling Policy.

Regular audits will be carried out to assess conformity to this Policy across the Council.

2.2 Records Management Principles

We manage records effectively as a strategic Council resource. Information resources, regardless of where they are held, are a corporate resource and hence the property of Lambeth Council and not the property of individual employees or teams. All information resources and processes must add value to the work of Lambeth Council and demonstrate value for money.

We are all responsible for the Council's records and information assets. Those with specific responsibility for managing particular information assets must be clearly identified. However, all users are accountable for their use of information.

We share records or information (responsibly) with our colleagues, partners and customers. Staff should be able to access information for the effective performance of their role and there should be the opportunity for the free flow of information, as appropriate, across Lambeth Council, partners and customers to support service outcomes.

We protect information, especially personal information, which cannot be shared for compliance reasons, for example in relation to data protection, security or due to commercial sensitivity.

We produce accurate information and meet our customers' expectations. Information must be timely, relevant, and consistent, with duplication of information kept to a minimum

We maintain our information in compliance with our statutory obligations. Information management must comply with prevailing legislation, information must be managed in accordance with Lambeth policies, standards and procedures and information must be kept as secure as appropriate.

2.3 Records Management Quality Criteria

Our Records must be:

- Accurate
- Timely
- Secure
- Fit for purpose
- Consistent
- Clear
- Usable
- Comprehensible
- Legally admissible as appropriate

2.4 Records Management Lifecycle

Records must be managed through their lifecycle: from creation, through storage and use, to disposal and archiving.

2.4.1 Record Creation

Information Asset Owners will:

- Ensure appropriate backup arrangements are in place for electronic records (including restoration of backups and disaster recovery if electronic records are damaged).
- Ensure all records created are necessary for a legitimate purpose or service delivery (data minimisation).
- Ensure adequate records are in place which document their area's activities.
- Ensure information is structured to facilitate shared working within the Council.
- Ensure that records are linked to metadata which documents their context and purpose.
- Records are appropriately referenced and classified in line with the Council's Information Protection and Handling Policy to enable the effective retrieval of information and help to secure access to sensitive records.
- Steps are taken to reduce unnecessary duplication of records.
- All record keeping systems in use have fully documented procedures and guidelines on the appropriate use of such systems.

Information Users will:

- Create, keep and manage information which will enable and record the Council's principal activities.

2.4.2 Maintenance

Information Asset Owners will ensure that:

- Adequate and appropriate storage for current records and semi current records and information is provided.
- Semi-current records and archive records are transferred in a controlled and appropriately secure manner to a designated record centre (on site or off site) or other central storage (e.g. for electronic records). This includes during office relocations when the risk of records being mislaid increases.
- Measures are put in place (where appropriate) to support the reuse of records and the information they contain, both internally and with partner organisations, where this is legally permitted and supports a legitimate aim of the Council or its partners.
- Procedures and practices are in place to protect records and information from loss in general, including loss or damage caused by fire, water, pest infestation, theft, unauthorised access or alteration.

- Procedures are in place to track the location and movement of structured records and information for easy retrieval and to provide an audit trail.
- Vital records and information are identified and safeguarded to support business continuity.

Information Users will:

- Maintain records the Council requires for business, regulatory, legal and accountability purposes.
- Create records with meaningful titles, indexes and metadata so that they can be retrieved quickly and efficiently.
- Make sure our records are accurate, reliable, have integrity and remain usable. This includes making appropriate arrangements for ensuring the continuity and availability of information when staff leave, or during major organisational or technological change.

2.4.3 Storage

To maximise efficiency, reduce costs, enable sharing and minimise risks Information Users will ensure that:

- Key business information should be stored in shared corporate repositories (e.g. SharePoint, Information@Work, Case Management Systems) most appropriate to the record.

Information should be stored securely, appropriate to its classification

- Service applications (e.g. Mosaic, Information@Work) should be used to store casework documents.
- Case related documentation should be stored where possible in a case management system or in electronic Document Management solution (eDMS) which is integrated into the case management system
- Information@Work or iDox should be used as the corporate eDMS and integrated into other business systems as required. Other eDMS solutions should not be procured unless agreed with the enterprise architect (design authority)
- All other documents should be saved on SharePoint or OneDrive, which are in Office 365.
- Work documents should not be kept on a computer desktop, local documents library, X- Drive.
- Documents saved on SharePoint and OneDrive are easier to access, share, and control. Keeping Council files on SharePoint and OneDrive will help to improve the quality and consistency of our document management.
- A SharePoint Team Site should be used to store and share team documents.
- A SharePoint Communication Site should be used to store and share documents relevant to all staff.
- A SharePoint Extranet Site should be used to store and share documents with partners
- OneDrive should be used to store and share private documents (e.g. HR files) or documents for temporary use.
- Microsoft Teams is a chat-based app linked to SharePoint. Any documents saved in Teams are automatically saved in a linked SharePoint Site, so feel free to use it to store and share documents.
- Dataset sharing between services, supported by information governance agreements within the council and between external partners should ideally be undertaken through system integration
- Storing duplicates should be avoided (e.g. avoid paper/electronic overlaps, e.g. store a single copy of electronic information to be shared through use of links) and routinely destroy temporary or draft material
- Records for permanent preservation should be transferred to the Lambeth Archives
- Information should not be stored permanently on removable media (e.g. DVDs, USB Memory Sticks)

Information Asset Owners will make appropriate contractual arrangements where information is stored, managed or hosted elsewhere on behalf of the Council in line with the Council's policies and applicable legislation.

2.4.4 Use

In order to balance the Council's commitment to openness and transparency and a desire to exploit our information whilst maintaining our responsibility for privacy and sensitivity, Information Users will:

- Ensure all Council records are subject to appropriate security measures as set out in our Information Security policy and other related policies.
- Document decisions regarding requests to access information ensuring they are consistent, can be explained and available for reference.
- Proactively publish information where it is considered to be in the public interest.

2.4.5 Retention and Disposal

The Data Protection Act does not set specific time limits for different types of data. LBL retention periods are documented in the **Lambeth Retention Schedule**. It is the responsibility of service areas to monitor these retention periods and identify any amendments required in line with specific needs or applicable legislation.

Lambeth Council shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

3. POLICY COMPLIANCE

All staff must comply with this policy as outlined in the Roles and Responsibilities Section. If you do not understand the implications of this policy or how it applies to you, seek advice from the Information Governance Team at InfoGov@lambeth.gov.uk.

Breach of this policy may be dealt with under the Staff Code of Conduct and Disciplinary Policy and Procedure and in serious cases, may be treated as gross misconduct leading to summary dismissal.

4. Supporting Procedures

See Lambeth Council Retention Schedule.

END