Wandsworth Council's Records Management Policy

Contents

1.0 Introduction

1.1 The Council creates, uses, and receives records which are a valuable resource and an important asset, supporting its legal, financial, business and administrative requirements. The systematic management of the Council's records, from creation to disposal, is essential to protect and preserve them as evidence of actions, to support present and future activities and business decisions, and to ensure accountability to present and future stakeholders. Furthermore, effective records management is central to upholding the Council's obligations under information legislation.

1.2 The Records Management Policy sets out the Council's commitment to consistently and securely create, keep, and dispose of high-quality records documenting its business and activities. It sets out the principles of good records management which shape the development of operational procedures. The policy also defines the characteristics of high-quality records, and describes the mechanisms of planning, governance and training that support compliance with the policy.

1.3 The purpose of the records management function is to:

- Create and capture authentic and reliable records which provide evidence of the Council's activities and decisions and which demonstrate its accountability.
- Secure, maintain and preserve those records for as long as they are required and to provide access to them as necessary to support the Council's operations and fulfil its statutory obligations.
- Identify those records which will form a significant part of the historical record of the Council's activities and make provision for their permanent or long- term preservation.
- Identify those records that are vital to the continuance of Council's business and protect them against disaster.
- Destroy records that are no longer required, having regard to statutory record-keeping requirements, thus promoting the efficient use of physical and electronic storage space, and negating malicious or accidental data loss.
- Respond to ad-hoc "legal hold" requests that may override default retention periods for particular records.

2.0 Legislative framework

The Records Management Policy has been created with reference to the following legislation and standards:

2.1 Legislation

- Care Act 2014
- Children and Families Act 2014
- Data Protection Act 2018 (DPA)

- Electoral Registration and Administration Act 2013
- Environmental Information Regulations 2004 (EIR)
- Finance Act 2020
- Freedom of Information Act 2000 (FOIA)
- General Data Protection Regulation (GDPR)
- Human Rights Act 1998
- Inquiries Act 2005
- Limitation Act 1980
- Local Government (Access to Information) Act 1985;
- Local Government Act 1972;
- Prevention of Social Housing Fraud Act 2013
- Public Records Act 1958 and 1967;
- Public Service Pensions Act 2013
- Regulation of Investigatory Powers Act 2000;
- Telecommunications (lawful business practices) and (interception of communications) Regulations 2000.
- Investigatory Powers Act 2016.

2.2 Standards

- ISO 15489 Information and Documentation – Records Management
- ISO 27001:2013 Standard for Information Security Management
- Section 61 Code of Practice on Records Management

2.3 The lists are not exhaustive and in addition managers need to identify and comply with legal obligations and professional standards pertinent to their business area and the information they capture, store, and use.

3.0 Intended audience

All members of staff are responsible for ensuring that records in their care are properly managed.

4.0 Scope

4.1 In records management it is important to be clear about the difference between a document and a record.

A document is any piece of written information in any form, produced or received by an organisation or person. It can include databases, website, email messages, word and excel files, letters, and memos. Some of these documents are ephemeral or of very short-term value.

Some documents will need to be kept as evidence of business transactions, routine activities or as a result of legal obligations, such as policy documents. These are official records.

In other words, all records start off as documents, but not all documents will ultimately become records.

4.2 For the purposes of this policy, a record is defined as:

Recorded information, regardless of media or format, created or received in the course of individual or organisational activity, which provides reliable evidence of policy, actions or decisions. (National Archives)

4.3 The Records Management Policy applies to:

- records created and received by all departments and/or services, in all formats, both paper and electronic
- records stored in any electronic or physical repository.

4.4 The Records Management Policy applies only to records, not to documents.

4.5 Records held by schools are the responsibility of the individual organisation and are outside of the scope of this policy. In the event of an organisation closing, the Council becomes responsible and liable for their records.

5.0 Policy statement

5.1 Effective management of current and historic records supports the business of the Council. In practice this means that:

- Accurate and robust record-keeping allows the Council reliably to identify people in need and provide them with the services they require quickly and efficiently, ensuring resources are directed where they are needed most.

- Good records management supports cost-effective and efficient business operations, freeing up valuable staff time to focus on the best possible frontline service delivery.

- By keeping records accurate and up to date, we ensure that reports on outcome indicators draw on authoritative information, thus supporting the Council to successfully achieve their targets.

- Sound recordkeeping practice supports partnership working with both service users and other public service providers, enabling productive working relationships while still protecting the Council against risks of information loss and/or unauthorised access to Council's information.

- Preservation and promotion of accessible historical records encourage local people to engage with the history of their communities, and generates learning opportunities for both young learners and adults. Public archive services also

enhance the positive image of the Council, promoting cohesion in local communities and encouraging visitor spend in the local areas.

- Identification of business-critical records and effective disaster management and preparedness regarding records and information are essential to ensuring the long-term sustainability of Council business.

5.2 The Council accepts the following core principles as essential to maintaining effective records management across the organisation. These principles apply to the management of all records, whether paper or electronic:

- Records management is recognised as a core corporate function.
- Records management policies and procedures are applied consistently across the Council.
- Records management is included in a governance framework with clearly defined roles and lines of responsibility.
- Records are mapped to business functions and activities.
- Records are created according to agreed forms and structures.
- Records are created with associated metadata, which is persistently linked and managed.
- Records are kept in systems that enable them to be stored, retrieved, used, and shared as necessary.
- Sufficient planning and resources are devoted to preserving records and making them accessible over time, particularly in the case of business-critical records.
- Records are maintained in a safe and secure environment, where access to them is controlled.
- Records are retained only for as long as they are required, and the Council can explain why records are no longer held.
- Record-keeping practice complies with legal and regulatory requirements, applicable standards and organisational policies, and compliance is regularly monitored and assessed.
- Proper arrangements are made for the long-term preservation of and access to materials of historic significance.

5.3 Records contain evidence of the Council's business transactions and/or information relating to those transactions. Records can also contain information the Council requires as part of its legal obligations. It does not matter what format the

record is in; a record can be an email, a file, a database, or any other format. What matters is the information the record holds.

5.4 In order to support business effectively, it is important to keep high quality records. To be considered 'good', a record should have the following characteristics:

- Authenticity: the record is what it claims to be and has not been tampered with. It can be relied on as evidence, for example in court.

- Reliability: the contents of the record can be trusted as a full and accurate representation of the Council's transactions and activities.

- Integrity: the record is protected against unauthorised alteration. Any authorised changes are clearly indicated and traceable.

- Useable: the record can be located, retrieved, presented and interpreted. Links between related records should be clear. It should be easy to determine what activity or department created the record.

6.0 Ownership

All records created and received by the Council, and its external service providers where they are processing information on the Council's behalf, who create, receive and use records, are the property of the Council, and must not be used for any activity or purpose other than official Council business.

7.0 Positions responsible for compliance

7.1 All staff who create, receive or use records will have some responsibility for their management. Specific responsibilities are outlined below.

- Information Governance Strategic Board (IGSB)

The Information Governance Strategic Board (IGSB) is made up of senior Information Governance and IT leads and has responsibility for the Information Governance and Security arrangements across the Shared Staffing Arrangement (SSA) that has been set up by Richmond and Wandsworth Councils. The IGSB's role is to drive forward delivery of the Information Governance Improvement Programme that is structured around the four work streams/service areas (including Information and Records Management) which form the basis of the Information Governance Framework. The IGSB also has oversight of compliance issues reported to it via the Information Governance and Security Forum.

- Information Governance and Security Forum (IGSF)

The IGSF is made up of key Information Governance and IT staff from across the SSA and Directorate Information Governance and Security representatives. It has a focus on operational aspects of Information Governance and compliance. In relation to Records Management the IGSF:

- Provides a corporate overview of all records management activities across the Council to ensure a consistent approach is followed to meet statutory requirements.
- Approves the Corporate Retention Schedule and ensures effective procedures and control mechanisms are in place for disposal of records or transferring records to off-site storage or the Council's permanent archives, as appropriate.

- Information Governance Manager

In the context of this policy, the Information Governance Manager is responsible for:

- Ensuring that the management of the Council's records complies with legal and professional obligations;
- Managing records in designated corporate records management systems;
- Advising Council officers on records management;
- Implementing the Records Management policy;
- Maintaining the Corporate Retention Schedule.

- Data Protection Officer

The Data Protection Officer (DPO) is responsible for advising, monitoring and reporting the Council's compliance with the General Data Protection Regulation (GDPR) and any relevant UK legislation (eg Data Protection Act). Formal duties are defined by the GDPR and include raising awareness of data protection requirements, leading information audits, advising on and reviewing data protection impacts and information sharing and investigating data breaches and incidents. The DPO is also the first point of contact for the Information Commissioner's Office and for individuals whose data is processed by the Council.

- Directorate Information Governance and Security Leads

Each Directorate has a nominated Officer who is responsible for disseminating information, instructions and guidance to the Directorate on behalf of the Information Governance and Security Forum (IGSF) and escalating any areas of concern to them.

- Information Asset Managers

Information Asset Managers are responsible for authorising the publication of the Council's data or information; authorising access to Council systems; granting access rights for their staff; ensuring that contingency plans and recovery procedures are in place to recover their business and operational processes; and ensuring that team members comply with information security policies.

- Information Asset Owners

Information Assets are identified and recorded on the Information Asset Registers. Information Asset Owners are nominated for all of the Council's Information. They are responsible for ensuring that: their systems are documented and managed appropriately to guard against operational failures; security requirements are

included in any changes to their system; only appropriate staff have access to their system and there are documented contingency plans for their system; any network links are protected appropriately and systems are protected against viruses; and system users are aware of their responsibilities for security and their system is monitored and audited to check for security breaches.

- Service Heads

All Service Heads, Business Unit Heads and Team Leaders will be responsible for ensuring:

- the records management policy is implemented and complied with in the department or service under their control;

- staff receive training, development and support in records management matters;

- all records within the department have an identified owner, responsible for their management whilst in use;

- adherence to proper procedures to ensure that no unauthorised destruction of records occurs, particularly any wilful destruction of records pertinent to a request made under the Freedom of Information Act, Environmental Information Regulations or the Data Protection (Subject Access Request) legislation;

- a satisfactory audit trail exists for records destroyed according to the retention and disposal schedules;

- records of long- term importance are offered to the Council's Local History/Archives Service for permanent storage;

- business recovery plans are in place to allow continuity of service in event of a disaster.

- Individual officers

All records created by officers during the course of their work are the property of the Council. Individual officers are responsible for:

- Adhering to corporate and any directorate records management policies;

- Filing records according to a file structure appropriate to their subject and format to enable ready retrieval when required;

- Ensuring that all records, regardless of format, are stored safely in suitable conditions;

- Ensuring that records are retained in accordance with the retention schedules and disposed of according to corporate and directorate policies when their retention period has expired.

- The Document Management Teams

The Document Management Teams provide scanning and indexing services for the Council.

7.2 Non-compliance could result in the Council being put at risk of legal challenge, service users being put at risk, colleagues being inconvenienced with their time wasted and Council resources being wasted.

7.3 Actions or neglect leading to a breach of this policy by an employee could result in disciplinary action.

8.0 Corporate Retention Schedule

8.1 The Corporate Retention Schedule has been created to support the Council to meet their statutory obligations to ensure that information is retained for the correct period and then disposed of appropriately.

8.2 It is unlawful to retain personal information for longer than necessary. If any delay is anticipated then this should be raised with the Data Protection Officer with a timescale for when the information will be disposed of.

8.3 The Corporate Retention Schedule sets out how long information should be kept before it is disposed of or, where it is deemed to be of permanent historical value, transferred to the Local History/Archives Service.

8.4 Staff should seek guidance from line managers in departments, or the Data Protection Officer, if they feel that any changes/ modifications/ additions to the schedule are required.

8.5 The Corporate Retention Schedule applies to any format that records and information may come in, digital or physical. Information that has reached the end of its retention period should be disposed of or transferred to the archive service without delay.

8.5.1 Documents are not covered by the Corporate Retention Schedule. They need to be destroyed as soon as they become obsolete.

In broad terms, documents are of a routine or trivial nature; have little administrative value, and only needed for a limited period.

Documents include, but are not limited to:

- copies of records used for reference purposes only.

- rough drafts of committee reports not circulated to other staff and of which a final draft has been produced and captured as a record. **NB**: Versions of drafts which contain significant changes to the context must be captured as records.

- E-mails giving minor instructions of a routine nature that are used to further some activity.

- working papers, background notes and reference materials used to prepare or complete other documents.

8.6 Any records destruction must be documented, either automatically by an audit trail, or manually be completing a Destruction Log. It is essential to take into consideration the format and the sensitivity of the information when deciding on the appropriate disposal method. When information is disposed of without an automated audit trail a Destruction Log shall be completed and forwarded to the Information Governance Manager so that sufficient descriptive details can be retained to enable accurate reporting on the information that has been destroyed.

8.6.1 Documents do not need to be registered in a Destruction Log.

8.7 Information may sometimes be kept in error because of technical problems, human error or by deliberate act. Information kept in error must always be reported, on discovery, to the information owner to allow them, in collaboration with the Data Protection Officer, to decide what action needs to be taken.

8.8 Wrongful disposal may occur because of technical problems, human error or by deliberate act. Wrongful disposal of information must always be reported, on discovery, to the information owner to allow them to identify any gaps in their information sets and to allow them, in collaboration with the Data Protection Officer, to take the decision as to what action needs to be taken and whether the Data Breach procedure needs to be instigated.

8.9 All staff, partners and contractors will adhere to the Council's Information Security Policies (as set out in the Information Security pages on the intranet) and, in relation to partners and contractors, any contractual or Data Sharing Agreement requirements, when disposing of or transferring information in any format including hardcopy, electronic and information contained on mobile storage devices.

8.10 The Corporate Retention Schedule indicates the sort of records that should be offered to the Local History/Archives Service. Where such a record is in electronic format, consideration should be given to the potential longevity of that format.

8.11 The Council's Archivist/Local History Officer will accept material that is no longer in active use where it has historical value. Material offered to the Local History/Archives Service will be appraised based on its historical value only.

8.12 The process of transferring information to the Local History/Archives Service must take into account the sensitivity of the information, and action must be taken to mitigate against loss of information during transfer.

8.13 Deletion policies for electronic systems:

8.13.1 SharePoint

Effective from January 1, 2024, newly created SharePoint sites will adhere to a standard deletion policy. This policy dictates that all items contained within these sites will be automatically deleted if they remain unmodified for a period of 6 years. SharePoint site owners are responsible for categorising their records by assigning retention labels to them. For further guidance on this process, please refer to the Records Management page on the Loop.

8.13.2 Outlook

Starting on January 1, 2024, all newly established Outlook mailboxes, whether shared or individual, will adhere to a uniform deletion policy. This policy stipulates that all emails within these mailboxes will be subject to automatic deletion after 6 years from their respective sent or received dates. Additional guidance on assigning retention labels to emails within Outlook can be found on the Records Management page located on the Loop.

Directors and Heads of Service will retain an exemption from automated deletions, unless they voluntarily opt-in to the policy.

9.0 Suspending the disposal of records

9.1 If a request (eg Subject Access Request) for access to information scheduled for disposal is received, the disposal action will be suspended pending a decision on its relevance to the request.

9.2 If the piece of information is subsequently used to answer the request, it needs to be retained for the remainder of the current year and a further 2 years.

9.3 The decision to interrupt a planned disposal and subsequent review of the information will be alerted to the information asset owner and undertaken by the information custodian in consultation with the relevant manager in their department (where applicable) or the Information Governance Manager.

9.4 The UK Covid-19 Inquiry has been set up to examine the UK's response to and impact of the Covid-19 pandemic and learn lessons for the future. Destruction of Covid-19 related records is suspended until further notice.

9.5 For advice or clarification on whether records are covered by the Inquiry retention hold the Information Governance Manager can be consulted.

10.0 Training and Awareness

As all Council employees are involved in creating, maintaining, and using records it is vital that they all understand their records management responsibilities as set out in this policy. Managers must ensure that all their staff are aware of their obligations

regarding Data Protection, Freedom of Information, and Records Management. Training on Information Governance and Security is mandatory for all staff.

11.0 Review

This policy will be formally reviewed every two years or more frequently if needed in response to a specific issue or requirement to ensure it continues to be relevant and current.

12.0 Related Documents

- The Corporate Retention Schedule can be found here: https://theloop.richmondandwandsworth.gov.uk/how-we-work/information-governance/records-management/

- Information governance advice can be found here: https://theloop.richmondandwandsworth.gov.uk/how-we-work/information-governance/

Records Management Policy

Document Name	Records Management Policy
Version No.	3.1
Status	Approved
Owner	Information Governance Manager
Approved by	Information Governance Strategic Board, 27 November 2023

If printed, copied or otherwise transferred from the Loop this document must be considered to be an uncontrolled copy.
Policy amendments may occur at any time and you should consult the Loop if in doubt.

Change Control Table

Version	Description	Who By	Release Date
1.0	**First approved version of the Records Management Policy.**	**IGSB**	**May 2019**
1.1	Draft reviewed version - feedback from IGSF members received and changes incorporated	SRMO	November 2021
2.0	**Second approved version of the Records Management Policy**	**IGSB**	**November 2021**
3.0	Draft reviewed version - feedback from IGSF members received and changes incorporated	SRMO	October 2023
3.1	**Second approved version of the Records Management Policy.** Minor amendments to paragraphs 2.1, 4.5 following comprehensive review. Main changes in paragraphs 8.13 and 9.4: Policy updated to reference the implementation of the Corporate Retention Schedule in electronic systems. Reference to IICSA removed, as Inquiry published its final report. Reference to Covid-19 Inquiry added.	**IGSB**	**November 2023**

Any queries with this document should in the first instance be brought to the attention of the document owner.

If this fails to resolve the problem in a timely manner then this should be escalated to the Head of Resident Engagement.