Wandsworth Council's
Records Management Policy

Table of Contents

1.Introduction

1.1 The Council receives and generates a large number of records which document and support its activities. These records are a vital source of information on its actions, policies and decisions.

1.2 The purpose of the Council's 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 obligations under the Freedom of Information, Environmental Information Regulations and Data Protection legislation;
- 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 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.

1.3 Robust procedures are required to ensure that the Council’s information assets are well managed and that we adhere to our statutory obligations. Having robust retention policies and procedures ensures that members of the public understand what information the Council holds, and for how long it is kept.

1.4 Stringent application of retention rules will also ensure that money is not being spent unnecessarily storing information; equally it will be easier to search for and find information, reducing the amount of resource needed to locate it.

2.Scope

2.1 For the purposes of this document, 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)

2.2 This policy covers all records created and received by all departments/service areas in any format, electronic or paper based. These will include:

- Service User records
- Photographs, slides and other images
- Microform (i.e. microfiche and microfilm)
- Audit tapes, cassettes
- Video tapes
- Record of staff – including payroll, personnel and administrative
- Computer media e.g. CD-Rom, Smartphones, removable storage (including USB sticks)
- Computer output
- Emails
- Digital records
- Scanned records
- Text messages (both outgoing from the organisations and incoming responses from the service user)
- Social media
- Administrative records including: personnel, estates, financial and accounting (e.g. budget information, annual report information)
- Information concerning complaint handling
- Manual (e.g. telephone messages, working papers)
- Printouts of audit trails from computer/automated systems

2.3 This policy applies to all the Council’s information and data sets, including those that the Council creates, holds on behalf of others or shares with third parties or partner organisations. All information, records and data sets including emails need to be stored in a manner that allows effective retrieval and allows the relevant retention rules to be applied.

2.4 Information asset owners must apply the policy whether within the Councils' environment, including SharePoint and OneDrive, or elsewhere.

2.5 Records held by schools are the responsibility of the individual organisation and are outside the scope of this policy.

3. Statement of Records Management Policy

3.1 The Council will implement and review procedures to ensure that reliable and usable records are created, maintained and made accessible for as long as they are required to support the business of the Council. This will be enabled by procedures to ensure that:

3.2 Records are managed in accordance with current legislation which includes:

- Data Protection Act 2018;
- General Data Protection Regulation, 2018 (GDPR)
- Freedom of Information Act 2000
- Environmental Information Regulations 2004;
- Human Rights Act 1998
- Local Government (Access to Information) Act 1985;
- Local Government Act 1972;
- Public Records Act 1958 and 1967;
- Regulation of Investigatory Powers Act 2000;
- Telecommunications (lawful business practices) and (interception of communications) Regulations 2000.

3.3 The list is not exhaustive and in addition managers need to identify and comply with legal obligations pertinent to their business area and the information they capture, store, and use such as:

- Children and Families Act 2014
- Care Act 2014
- Finance Act 2014
- Public Service Pensions Act 2013
- Electoral Registration and Administration Act 2013
- Prevention of Social Housing Fraud Act 2013

3.4 Records are managed in accordance with current professional standards. These include in particular ISO 27001:2013 (Standard for Information Security Management), accreditation for which has been achieved by the Council.

3.5 Managers also need to identify and comply with professional standards pertinent to their business/service area and ensure that:

- Records management practices are compatible with corporate procedures relating to search and disclosure (Freedom of Information, Data Protection, fraud and criminal investigation, staff or contractor malpractice)

- Records are accessible to officers to support them in making informed and proper judgments in the course of their work;

- Records are accessible to the public in accordance with the Councils' Publication Scheme, the Transparency Code and the requirements of the Freedom of Information Act, 2000; and the Environmental Information Regulations, 2004.

- Records are kept securely and protected from accidental or deliberate loss or destruction;

- Records are maintained in a secure environment with good conditions for their physical preservation and storage and which allows access as needed;

- Records are kept in accordance with the schedules drawn up for their retention, having regard to legal requirements and recognised good practice, and are safely disposed of after the expiry of their retention period in accordance with legal and regulatory obligations;

- All staff are aware of their obligations in respect of the filing, retention and disposal of records.

- Documents are named in a consistent manner and those setting out policies, procedures and guidance to staff include the 'version control' template which is available on the Intranet. This helps to ensure users are looking at the current version of the document and identifies its 'owner' as well as the approving body and date of most recent approval. Only authorised persons will have the right to amend or distribute such documents. This helps to create an audit trail of how the document has changed over time and why.

4. Ownership

4.1 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.

5. Active Management of Information

Data

- Information held in databases, including share point sites, is constantly evolving, however this does not mean that it is exempt from the records management policy. Information owners must ensure that information held in databases meets our statutory obligations with regard to retention and disposal. Defunct or closed databases must be managed in accordance with the retention and disposal schedule.

- The Council will take active steps to ensure that the information held in databases it manages, owns or use is accurate and up to date and not retained beyond the time limit set out in the retention and disposal schedule. Where there seems to be no justified reason to hold personal or sensitive information it must be destroyed immediately, unless the information asset owner can present a sound business reason or statutory requirement to the Data Protection Officer.

- In managing information held in databases the Council will correct errors on discovery and dispose of out of date records in line with the corporate retention and disposal schedule. Information collected in error or found to be a duplicate will be deleted.

- Where information needs to be retained for statistical or research purposes the information owner must ensure that all such information is anonymised or meets our statutory obligations for the management of personal or sensitive information.

Email

- Emails and attachments relating to Council business are corporate records and must be managed in accordance with the Council's retention and disposal schedule.
- Email users need to manage their accounts effectively and proactively and retained emails should be filed appropriately.

Future Considerations

Retention of records must be incorporated into the statement of requirements for the procurement of any new system. Retention capabilities must be installed on any new system as a pre-requisite to go-live.

6. Disposal of information

6.1 Information that has reached the end of its retention period should be disposed of or transferred to the Local History/Archive Service without delay.

6.2 It is essential to take into consideration the format and the sensitivity of the information when deciding on the appropriate disposal method. It is essential that paper information that is sensitive, or if it has potential legal repercussions or a high risk of reputational damage to the Council, is placed in the confidential waste bins to ensure the information is disposed of securely. Examples of this include information regarding personal data or potentially commercially sensitive information.

6.3 Electronic information must be treated in the same way as physical information; therefore, electronic information must be disposed of once it has reached its set disposal date.

6.4 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.

6.5 Information may sometimes be kept in error as a result 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. If the decision is taken to alter the retention period, a sound business reason needs to be approved by the relevant Head of Service, Assistant Director or Director and the Data Protection Officer.

6.6 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.

7. The Role of the Retention and Disposal Schedule

7.1 The retention and disposal schedule helps the Council to meet its statutory obligations to ensure that information is retained for the correct period of time and then disposed of appropriately. It is unlawful to retain information for longer than necessary.

7.2 The 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. 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. Principles of Retention

8.1 Information is assessed and a retention period set according to the following principles:

Statutory requirements: information will be retained for only as long as is required by statute.

Ongoing business need: information will be retained for only as long as it is required to run the organisation effectively. Storing information costs money, therefore storing information for longer than is necessary incurs unnecessary costs.

Best practice: information will be retained if best practice indicates this would be of benefit, best practice can be drawn from respected external sources.

8.2 When the retention period is complete a decision must be made by the information owner to dispose of the information, or to offer it to the Local History/Archives Service if it is deemed to be of permanent historical value (see section 9).

9. Transfer of Records of Historic Interest to the Local History/Archives Service

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

9.2 Information offered to the Archives Service is not always kept and may be weeded or sampled to reduce the quantity. Therefore, only information that has reached the end of its retention period should be offered to the Archives Service.

9.3 The process of transferring information to the Archives Service must take into account the sensitivity of the information, and action must be taken to mitigate against loss of information during transfer. The Council will develop processes for the safe transfer of information to the Archives Service.

9.4 The Retention and Disposal schedule indicates the sort of records that should be offered to the Archives Service with contact details for the service. Where such a record is in electronic format, consideration should be given to the potential longevity of that format.

9.5 Information not required by the Archives Service must be disposed of in accordance with section 8 of this policy.

10. Recording of information that has been disposed of

10.1 When information is disposed of a Document Destruction Log shall be completed and forwarded to the Information Governance Manager so that the Council can retain sufficient descriptive detail to enable accurate reporting on the information that has been destroyed.

11. Suspending the disposal of records

11.1 If a request (eg Data Protection Act 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.

11.2 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.

11.3 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.

12. Information wrongly disposed of

12.1 Wrongful disposal may occur as a result 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 also 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.

12.2 The information owner will investigate the circumstances surrounding the wrongful disposal. The results of this investigation will be reported to and agreed by the relevant Head of Service, Assistant Director or Director. Where appropriate, procedures will be changed in order to ensure further disposals in error cannot take place, or that such a risk is mitigated.

12.3 If the wrongful disposal may have resulted in a data breach, a security incident report (available in the Information Security pages on the Loop) should be completed without delay.

13. Representation, Roles and Responsibilities

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

Information Governance Strategic Board

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 Councils' 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 corporate retention and disposal schedules.

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 Councils' 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 Councils'

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. They are also responsible for the management of the off-site storage contract, co-ordinating the despatch and retrieval of records sent to off-site storage and ensuring that records are destroyed securely when their disposal date is reached.

14. Training and Awareness

14.1 The Council recognises the importance of good records management and has implemented a programme of training to ensure that all officers are aware of their duties and responsibilities in this respect. Certain training on Information Governance and Security is mandatory for all staff.

15. Management and Review

15.1 Service Heads and managers are responsible for ensuring compliance with all corporate policies.

15.2 Compliance with this policy will be monitored by the Information Governance Manager in collaboration with Directorate Information Governance and Security Leads.

15.3 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.

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

15.5 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.

Records Management Policy

Document Name	Records Management Policy
Version No.	1(May 2019)
Status	Approved
Owner	Information Governance Manager
Approved by	IGSB/IGSF on 19 and 26 March respectively.

If this document is in printed format it may not be the current version. Before subsequent use check the documents version number on the intranet.

Document Control

This document should be reviewed annually by the document owner and a note made to this effect in the table below

Change Control Table

Version	Description	Who By	Release Date

Any queries with this document should in the first instance be brought to the attention of the document owner whose names appear on the front page.

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