Corporate Records Management Policy

Status

Final 1.0

Issued by the Corporate Team, Legal Services

Document Classification

Privacy & Data Protection

Document History

Issue	Change	Changed By	Authorised By
Draft 0.1	Initial Draft – No changes		
Draft 0.2	Incorporate comments from RMU	Norman Coombe	
Draft 0.3	Incorporate comments from Distribution list	Norman Coombe	
Draft 0.4	Incorporate comments from Distribution list	Norman Coombe	
Draft 0.5	Incorporate comments from Senior Lawyer	Norman Coombe	
Final 1.0			

Distribution / Actions

Name	Job Title	Action
	Departmental Records Managers	For comment
	Head of Data Security	For review & comment
CGP		For review & comment
SIRO		For sign-off

Final distribution

This policy is available to all Southwark employees and Council members through The Source. Hard copies for distribution may be requested through the Corporate Freedom of information Officer.

1. Introduction

Southwark Council holds a large amount of information. This information may relate to specific topics or individuals as well as records of decisions made by the Council, actions taken and the rationale behind these decisions. The Council recognises that its records are an important public asset, and are a key resource to effective operation, policy-making and accountability. Like any asset, records require careful management and this policy sets out the Council's responsibilities and activities in respect to this.

2. Scope

The purpose of this document is to define the elements of the Council's records management policy.

All employees of the Council have a responsibility to effectively manage Council records in accordance with specified legislation and guidelines (see appendix 1).

A record is defined as any information held by the Council regardless of medium (including paper, microfilm, electronic, audio-visual and record copies of publications), which is created, collected, processed, used, stored and/or disposed of by the Council, its employees, and by those acting as its agents in the course of a Council activity.

3. Objectives

The aim of this policy is to define a framework for managing the Council's records.

When it comes to looking after our information there are five simple principles:

Keep it safe

We are all responsible for looking after council information so that it is kept secure and confidential but accessible to those of us who are authorised to use it for day to day business.

Keep it current and accurate

It is everyone's responsibility and part of our daily business routine to keep all types of information accurate and up to date. All essential paper records not used regularly must be archived offsite or in a suitable electronic format for no longer than the agreed retention period.

Save it electronically

We store our information electronically, unless there is a legal reason to keep it in another format.

Share it

Information we create and receive belongs to the council and is a shared strategic asset.

Managers are responsible for making sure that staff who leave or join departments understand how to manage information and that their security permissions are updated accordingly. Managers will cooperate with colleagues and partners to ensure that in

appropriate circumstances and where there is a proven need and robust safeguards, information is able to be shared and utilised for the benefit of Southwark residents.

Remember with personal data any sharing must be in line with an Information Sharing Protocol or in compliance with our responsibilities under the Data Protection Act.

Know the law

We must all be aware of the latest legislation that governs how we deal with the information used in our business operations.

4. Identification of roles and responsibilities

The Strategic Director of Finance and Corporate Services will have overall responsibility for information governance and records management practices.

The Director of Legal Services will be responsible for compliance with Freedom of Information requests, Data Protection requests, the publication scheme, records management practices and will co-ordinate activities such as maintaining the corporate retention schedule.

The Head of Corporate team, Legal Services will be responsible for legal advice relating to any of the above and will be responsible for maintaining the corporate retention schedule

Strategic Directors are responsible for the management of their own records, in accordance with this policy, and for ensuring that their staff are aware of record keeping issues and training.

Led by the Strategic Director of Finance and Corporate Services, the Council Management Team will have responsibility for developing positive behaviours and culture of proactive management of records.

All Council employees will be responsible for creating and maintaining records in relation to their work that are authentic and reliable. There should be staff with specific responsibilities for records management in each department.

5. Records Creation and Record Keeping

Departments must put in place adequate records management procedures, including measures to ensure that working records about people are fair, accurate, up-to-date and not excessive. Records about people must be secure, traceable and accounted for at all times. Records management procedures, including retention and disposal, apply equally to paper and electronic records including emails.

All information assets should be clearly identified and an inventory of all important assets drawn up and maintained.

The asset inventory should identify all assets and document the importance of these assets including all information necessary in order to recover from a disaster, type of asset, format, location, backup information, licence information and a business value.

Ownership and information classification should be agreed and documented for each of the assets.

Each department should have in place a record keeping scheme (paper or electronic) that documents its activities and provides for quick and easy retrieval of information. It must also take into account the legal and regulatory environment specific to the area of work.

6. Record Maintenance

The record keeping system must be maintained so that the records are properly stored and protected, and can easily be located and retrieved. This will include:

- Ensuring that adequate storage accommodation, both on site and off site, is provided for the records.
- Tracking and monitoring the movement and location of records so that they can be easily retrieved (This provides an audit trail).
- Controlling access to the information.
- Identifying vital records and applying the appropriate protection, including a business recovery plan.
- Ensuring non-current records are transferred in a controlled manner to the council's offsite storage provider, Archival Records Management (ARM).
- Rules for the acceptable use of information and assets associated with information processing facilities should be identified, documented and implemented

7. Access Control

The Council needs to ensure that any decisions regarding access to the records are documented so that they are consistent, and can be explained and referred to.

Strategic Directors must ensure that:

- All staff are aware of the arrangements for allowing access to certain types of information.
- Procedures are in place to document decisions concerning access.

All employees, contractors and third party users should follow rules for acceptable use of information and assets associated with information processing facilities

Files, including case work, must not be left on the desk unattended. If you are away for an extended period (½ hour or more is a guide), for example attending a meeting, you must clear your desk of all confidential materials and put them away in a secure designated cupboard. There is a balance to be struck in putting away files for the duration and effectively completing your duties. If you are away from your desk at any time all files should be closed. At the end of your working day you should clear all materials from your desk.

Any boxes or folder with sensitive information or otherwise, are not to be left on or underneath desks or in meeting rooms. They should be put away in the secure cupboards provided on the floor. Generally you should, have only the files you are currently working on at your desk.

Case files are to be placed in the cupboard and in the appropriate location as agreed by your line manager/team protocols to ensure none are misplaced or 'lost'. No case files or sensitive materials are to be kept in personal lockers under any circumstances.

Ensure that all cupboards and file locations where sensitive information is held are locked and secure at all times. . Ensure that access is restricted to those who require the information and a procedure put in place to secure access rights.

8. Record Retention and Disposal

As part of conducting normal business for Southwark Council, we create and receive records, which are important council assets. These records can exist in various formats, such as paper and microfilm or fiche, and also electronic. Electronic records can include Microsoft Word documents, spreadsheets, emails and digitised or scanned documents or images and records held on data systems.

We have legislative obligations to retain some of these records for set periods of time, under various Acts of Parliament or statutory instruments.

Other records may need to be retained for a certain time period because we know there is a business requirement to do so.

Records of continuing value, which are no longer required to be accessed regularly or quickly, should be transferred to storage using the council's offsite storage provider ARM.

To find out how long you need to retain every type of record you might create as part of your daily business, go to the retention and disposal schedule on the Source.

Retention and Disposal of Records

The retention and disposal schedule is the document and legal authority, that specifies how long we need to retain each type of record, and also when and how they should be disposed. It applies to both physical and electronic records. The retention and disposal schedule has been reviewed and authorised by representatives from all departments within the Council.

Disposing of records which are no longer required, either for legal or business reasons saves both space and money. Business units must pay for the cost of records storage, boxes and for the storage and transfer of records to the offsite storage facility. We should not pay for space to store records which are no longer useful or legally required, whether they are physical or electronic records. Disposing of records which are no longer required can reduce the size and cost of storage space we require considerably.

With regard to electronic records staff should ensure these are kept no longer than necessary for the purpose in order to comply with the fifth data protection principle.

Before you dispose of council records, you must refer to the retention and disposal schedule and records must be disposed of securely in accordance with it. Regular disposal of records is considered good information management practice, and should become part of your normal administrative practice.

9. Review of Policy

This policy will be reviewed in conjunction with the Freedom of Information Act Publication Scheme every two years.

Appendix 1: Standards, Legislation and Council Policies

- Public Records Act 1958 and 1967
- Local Government (Records) Act 1962
- Local Government Act 1972
- Local Government (Access to Information) Act 1985
- Data Protection Act 1998
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Records Management Standards and guidelines
- British Standards (BSI)
    - BS 4783 Storage, transportation and maintenance of media for use in data processing and information storage
    - BS 7799 Code of practice for information security management
    - BS ISO 15489 Information and Documentation - Records Management
    - BSI DISC PD0008 Code of practice for legal admissibility and evidential weight of information stored on electronic document management systems
    - BSI DISC PD0010 Principles of good practice for information management
    - BSI DISC PD0012 Guide to the practical implications of the Data Protection Act 1998
    - BS ISO IEC 27002:2005 Code of Practise for Information Security Management

- Records Management Society of Great Britain - Retention Guidelines for Local Authorities 2003

- Ministry of Justice: s46 Code of Practice

- LBS: Data Protection Policy