



HILLINGDON

LONDON

Document Retention and Destruction Policy

Contents	Page
1. Introduction	2
2. Scope	2
3. Purpose	2
4. Policy	3
5. Roles and Responsibilities	3
6. Document Management Framework including Electronic Records	4
7. Performance Management	7
8. Promotion, Training and Support	7
9. Review Cycle	7
Appendix A - Relevant Policies and Legislation	8
Appendix B - Retention and Destruction Schedules for Directorates	9

Version	Amended by	Date	Summary
1.0		May 2018	
2.0		May 2023	

1. Introduction

- 1.1 The London Borough of Hillingdon ('The Council') holds information including (but not limited to) personal and special category information about residents, employees and other corporate information. The Council recognises the importance of its records, which are a key resource to effective governance, service planning, financial management and performance management. It is therefore important that information is well-managed and used effectively to deliver and improve services. This policy sets out the Council's responsibilities in respect of the retention and destruction of its records.
- 1.2 The Council has a statutory responsibility to retain and destroy all of its records in accordance with the requirements of the Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR), other relevant legislation and recognised guidelines.
- 1.3 This policy covers all information, whether held in notes or structured records systems (paper and electronic), which were received or created by the Council in the course of its business. Although not exhaustive, examples of records include:
- Documents (including hand-written, typed and annotated copies);
 - Paper based files;
 - Computer files (including word documents, databases, forms, reports, spreadsheets and presentations);
 - Emails
 - Maps and plans;
 - Web pages on the intranet;
 - CCTV images and audio recordings of telephone calls to specific service areas.

2. Scope

- 2.1 This Document Retention and Destruction policy aligns with the 'storage limitation principle' under Article 5(1)(e) of UK GDPR which states that personal data shall be kept in a form which permits identification of individuals, for no longer than is necessary (for the purposes for which the personal data are processed).
- 2.2 This policy also ensures the Council complies with the 'data minimisation' and 'accuracy' principles under Article 5(1)(c) and (d) of UK GDPR and other requirements, referenced in **Appendix A**.
- 2.3 This Policy applies to:
- 2.3.1 All Employees of the Council;
 - 2.3.2 Members of the Council;
 - 2.3.3 Temporary and Agency Staff engaged by the Council;
 - 2.3.4 Volunteers at the Council;
 - 2.3.5 All others using the Council's Information or Systems.

3 Purpose

- 3.1 The aim of this policy is to ensure that managers and their teams retain records in line with the Retention and Destruction Schedules set out in **Appendix B**.
- 3.2 This policy provides clarity about:

- a) Roles and responsibilities for managing the retention and destruction of records;
- b) Which type of records should be retained and for how long;
- c) The storage arrangements for paper records which need to be retained; and
- d) The arrangements for the destruction of records which are no longer required.

4 Policy

- 4.1 Records should only be retained where there is a justifiable business need and/or statutory need to retain the record. The Data Protection Act 2018 and the UK GDPR sets out that personal data shall not be kept for longer than is necessary for its purpose(s).
- 4.2 Where records need to be retained, they should be retained for only as long as is defined in legislation and/or guidance. Records should be retained securely, protected from risk of damage and deterioration and in an organised manner. This includes electronic and paper-based records. Where records include confidential or sensitive/special category information, these records need to be stored securely with access controls in place.
- 4.3 When records no longer need to be retained (in accordance with the Retention and Destruction Schedules set out in **Appendix B**), they should be permanently destroyed, in a secure manner. This includes paper and electronic parts of the same record, where these exist. Confidential and sensitive/special category records should be permanently destroyed in a secure way to prevent future access to these records.

5 Roles and Responsibilities

Senior Information Risk Owner (SIRO)

- 5.1 The SIRO is responsible for periodically reviewing and updating the Document Retention and Destruction Policy and Retention and Destruction Schedules for Directorates.

Heads of Service

- 5.2 The Heads of Service are responsible for agreeing which records need to be retained and destroyed, as set out in the Retention and Destruction Schedules for Directorates (Appendix B) for their particular service area. They also agree changes to the schedules for their service areas.

Service Managers

- 5.3 The Service Managers are responsible for ensuring compliance with this policy and the Retention and Destruction Schedules for Directorates at Appendix B. Service Managers to review the Retention and Destruction Schedules for their service areas and advise their Heads of Service of any changes which need to be made to these Schedules. Service Managers to ensure that where records (electronic and paper) need to be retained, they are stored in line with the Retention and Destruction Schedules for Directorates at Appendix B. Service Managers to arrange the destruction of records, which no longer need to be

retained in line with the Retention and Destruction Schedules for Directorates at Appendix B.

Service Areas

- 5.4 The designated points of contact in the Service Areas are responsible for managing requests from Service Managers to store and retrieve records from the Councils external storage provider for the storage of paper records. Each service area will regularly review requests for records storage and the retrieval of records, to ensure they are minimising the cost of managing paper based records. The service areas are also responsible for scanning and storing electronic records on the Council's systems.

All Staff

- 5.5 All members of staff have a responsibility to ensure effective management of records in accordance with data protection principles. Staff with specific responsibilities for records management should have these clearly defined in their job descriptions and adhere to this policy and schedules.

Council's external storage provider

- 5.6 MJF Records Management is the Council's external storage provider, which is tasked with the storage, retention and destruction of off-site Council records. The MJF user guide on the intranet provides details about the procedure in place to arrange external storage. Further information should be sought from Sean Stone in Building Services Team.

6 Document Management Framework including Electronic Records

6.1 Retention and Destruction Schedules for Directorates

- 6.1.1 The Retention and Destruction Schedules for Directorates at Appendix B have been agreed by the Senior Management Teams across the Council. The Service Managers should ensure that they consult the Retention and Destruction Schedules for Directorates at Appendix B to identify the relevant retention period. They then need to decide the format in which the records should be retained. For records held in paper format, the Service Managers should determine whether the paper format should be held with the Council's external storage provider or alternatively scanned and held electronically within the Council's systems. The Service Managers will need to take into account that records originally held in paper format (which are subsequently scanned and held electronically within the Council's systems), will either need to be permanently destroyed in their entirety (where appropriate) or retained in part in paper format where there are original legal/official documents.
- 6.1.2 Each Service Area should have in place a record keeping system (paper and electronic) that documents the description of the records held, for whom they relate to, the location of such records (as to whether they are held with the Council's external storage provider or held electronically within the Council's systems) and any decisions relating to securely destroying/retaining original legal/official documents (if relevant).
- 6.1.3 It must also take into account the legal and regulatory environment specific to

the area of work. This record keeping system will include:

- Records arranged and indexed in such a way that they can be retrieved quickly and efficiently;
- Procedures and guidelines for referencing, indexing, version control and security marking;
- Procedures for keeping the system updated;
- The ability to cross reference electronic and paper records; and
- Documentation of this system and guidelines on how to use it.

6.1.4 They should be aware of the general principles that where there is no statutory requirement to keep records for a specified period of time, the Council will destroy the record after 6 years (plus current year) in accordance with the Limitation Act 1980. In circumstances where a specific statutory requirement or business need applies, this should be adhered to. The retention periods are set out in the Retention and Destruction Schedules for Directorates at Appendix B.

6.2 Record Maintenance

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

- Ensuring that adequate storage accommodation is identified for the records;
- Tracking and monitoring the movement and location of records so that they can be easily retrieved (therefore providing an audit trail);
- Controlling access to the information;
- Identifying vital records and applying the appropriate protection, including a business recovery plan; and
- Ensuring records that are not required to carry out a current workstream are electronically scanned, with original documents retained and stored with the Council's off-site archive provider only where there is a business/statutory reason for doing so. This should take into account the costs implications of storing paper records and such decisions shall be determined by Service Managers.

6.3 Storing and Retrieving Records

6.3.1 When submitting a paper record for storage, the Service Manager must ensure that the proper process has been adhered to.

6.3.2 Only Service Managers and above can request that records are stored with the Council's off-site archive provider. As a minimum, the following information must be provided (or the record will not be accepted for storage):

- Case reference number;
- Description of record;
- Location of any related original paper legal/official records;
- Name of service user/employee;
- Manager/Officer contact;
- Destruction date and

- Team/Service area.

6.3.3 There is a financial cost to the Council to retrieve paper records from storage. Only Managers and above can request that paper records are retrieved from storage. In circumstances in which access to a paper record is likely to be required on a regular basis, the Manager should consider making arrangements to store the paper records locally on a temporary basis to reduce the cost of retrieving these records to the Council.

6.3.4 Requests to store and retrieve paper records with the Council's external storage provider can be made through designated points of contact within service areas, with the exception of children social care records which are kept and managed by their Business Support Unit. The provider will not accept requests directly from all staff.

6.4 Destroying Records

6.4.1 With increasing public access to our records, it is important that disposal of records happens as part of a managed process and is properly documented. Therefore, service areas must have in place clearly defined arrangements for the assessment and selection of records for disposal, and for documenting this work. Managers are responsible for identifying and authorising the destruction of records which no longer need to be retained. This includes electronic records and paper records. Confidential paper records, including personal and sensitive/special category data must be destroyed in a secure way using confidential disposal facilities.

6.4.2 For paper records stored by the Council's external storage provider, the provider will destroy the records securely on behalf of the Council when the record reaches its designated destruction date (as requested by the service areas), unless the relevant Service Manager advises that the records should not be destroyed.

6.4.3 Paper records also include reports, manuals, working papers and papers for meetings. Where these no longer need to be retained, they should be destroyed, including papers held in filing cabinets etc.

6.4.4 For records held electronically, Managers will need to ensure that their teams are only retaining electronic records in line with the schedules at Appendix B. This includes electronic information held on shared drives, information published on the Council's intranet and email accounts.

6.4.5 For electronic case records, Managers will need to liaise with the ICT team to make arrangements to destroy electronic records, as and when appropriate.

6.5 Access

6.5.1 The Council needs to ensure that any decisions regarding access to the records are documented so that they are consistent in their approach and can justify the reason. Managers must ensure that:

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

7 Performance Management

7.1 The Building Services Team manages the contract for the Council's off-site storage provider. Hillingdon Information Assurance Group (HIAG) monitors the performance with regard to the storage, retention and retrieval of Council records. Indicators will include:

- Response times of the off-site storage provider in providing information;
- Customer satisfaction surveys of the off-site storage provider.

8 Promotion, Training and Support

8.1 As all Council employees are involved in creating, maintaining and using records, it is vital that they all understand their record management responsibilities as set out in this policy. Managers will ensure that staff responsible for managing records are appropriately trained or experienced and that all staff understand the need for records management. Managers must ensure that all their staff are aware of their obligations regarding Data Protection, Freedom of Information and Records Management.

8.2 For further information about this policy please contact the Council's Statutory Data Protection Officer:

Glen Egan, Acting Head of Legal Services and Monitoring Officer
E-mail: gegan2@hillingsdon.gov.uk Telephone: 01895 277602

For further information about the Council's external storage provider, please contact:

Sean Stone, Soft Services Manager
E-mail: sstone1@hillingsdon.gov.uk Telephone:

9 Review Cycle

9.1 The Council's Document Retention and Destruction Policy will be updated periodically (as and when required) and be subject to a detailed review every 3 years to ensure it is up to date with best practice in this area. The next detailed review is planned for May 2026.

Appendix A

Relevant Policies and Legislation

Relevant Council Policies

- Information Governance Policy;
- Data Protection Policy;
- Data Protection Individuals' Rights Policy;
- Lawful Basis for Processing of Personal Data Policy.

Relevant Standards and Legislation

- Local Government Act 1972;
- Local Government (Access to Information) Act 1985;
- Freedom of Information Act 2000;
- Records Management Standards and guidelines;
- UK General Data Protection Regulation (EU) 2016/679;
- Data Protection Act 2018

Appendix B

Retention and Destruction Schedules for each Directorate

This is available on the Intranet as a separate PDF document.