Document Retention and Destruction Policy

MAY 2018

HILLINGDON
LONDON

Contents

The key contacts in connection with this policy are:

Muir Laurie
Senior Information Risk Owner and Head of Business Assurance
t: 01895 556132
e: mlaurie@hillingdon.gov.uk

Raj Alagh
Borough Solicitor and Statutory Data Protection Officer
t: 01895 250617
e: ralagh@hillingdon.gov.uk

1. Introduction

1.1   The London Borough of Hillingdon (LBH) 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, policymaking and accountability. Like any asset, records require careful management and this policy sets out the Council's responsibilities and activities in respect to this.

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 General Data Protection Regulation (GDPR) and other relevant legislation and recognised guidelines. Records can be defined as information, recorded in physical form or medium, received or created by the Council in the course of its business and retained as evidence of its activities or because of the information contained in them will be useful for others. Although not exhaustive, examples of items that can constitute records include:

- Documents (including hand-written, typed and annotated copies);

- Paper based files;

- Computer files (including word processed documents, databases, spreadsheets and presentations);

- Maps and plans;

- Email, web pages (on either the intranet and internet) and faxes;

- Brochures and reports;

- Forms; and

- Audio and video tapes including CCTV and voicemail/voice recording systems.

2. Scope

2.1   This Document Retention and Destruction policy aims to provide guidance for the creators and users of Council records and information in order to provide the most effective business processes and service delivery and to meet Council and legislative requirements (refer to **Appendix A**).

2.2   The Chief Executive, the Corporate Management Team (CMT), Senior Management Teams (SMTs), Members of the Audit Committee, Members of Cabinet and Full Council should all be familiar with this policy. This document applies to all employees of the Council, with the exception of Hillingdon schools which are required to put in place their own retention and destruction arrangements.

3. Purpose

3.1   The aim of this policy is to ensure that managers and their teams retain only those records they are required to. This policy provides clarity about:

a) Roles and responsibilities for managing the retention and destruction of records;

b) Which 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 legal need to retain the record. The Data Protection Act 2018 and the 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 in an appropriate way, protected from risk of damage and deterioration, and efficiently accessible to anyone who has the right to access them. This includes electronic and paper based records. Where records include confidential or sensitive information, these records need to be stored securely.

4.3   When records no longer need to be retained (in accordable with the guidelines) they should be destroyed. All elements of the record should be destroyed which includes paper and electronic parts of the same record where these exist. Confidential and sensitive records should be destroyed in a secure way to prevent future access to these records.

5. Roles and Responsibilities

Senior Information Risk Owner and Head of Business Assurance

5.1   Responsible for periodically reviewing and updating the records retention and destruction policy and guidelines.

Heads of Service/Deputy Directors

5.2   Responsible for agreeing which records need to be retained and destroyed as set out in the records retention and destruction schedule for their particular service area. They also agree changes to the schedule for their service area.

Service Managers

5.3   Responsible for ensuring compliance with the policy and records retention/destruction schedule. Service Managers review the schedule of records to be retained and advise of any changes which need to be made to the records retention guidelines which affect their service area or other service areas. Managers ensure that where records need to be retained, they are stored as long as is necessary according to the records retention/destruction schedule (this includes paper and electronic records). Managers destroy records which no longer need to be retained.

Business Support

5.4   Are responsible for managing requests from Service Managers to store and retrieve records from the Councils agreed provider for the storage of paper records. Business Support Units will regularly review requests for records storage and the retrieval of records to ensure that we are minimising the cost of managing records.

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.

Restore

5.6   Restore is the Council's external storage provider which is tasked with the storage, retention and destruction of off-site Council records. These records are currently stored at a facility near Newcastle.

6. Document Management Framework inc Electronic Records

6.1   Records Retention

6.1.1   For some records, there is a requirement to retain the record for a minimum period for future reference. The need to retain and store records will fall into the following categories:

Category	Action
No requirement to retain the record	Destroy record, refer to section 6.4.
Retain for a fixed period of time	Refer to schedules by Directorate
Permanent storage/archive	Refer to schedules by Directorate

6.1.2   As a guideline for managers, the retention schedules broken down by Group (Directorate) sets out periods of time that records should be retained, for different types of records. These Retention Schedules match the needs identified by Service areas in the recent data mapping exercise.   Where records need to be retained, it is important that managers ensure that all elements of the electronic record are stored in one place for ease of retrieval at a later date. This includes email correspondence where this is part of the record.

6.1.3   Each service should have in place a record keeping system (paper and electronic) that documents its activities and provides quick and easy retrieval of information. It must also take into account the legal and regulatory environment specific to the area of work. This system will include:

- Records arranged and indexed in such a way that they can be retrieved quickly and efficiently;

- Procedures and guidelines for referencing, titling, indexing and 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.
- Where there is no statutory requirement to keep records for a specified period of time, the Council will destroy the record after 6 years in accordance with the Limitation Act 1980. Where a specific statutory requirement or business need applies, this is shown in the attached schedules.

6.2   Record Maintenance

6.2.1   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 is provided 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 non-current records are transferred in a controlled manner to a designated records centre rather than stored in offices.

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 specialist service provider. As a minimum that the following information must be provided (or the record will NOT be accepted for storage):

- Case reference number;

- Description of record;

- Name of client;

- 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 Service 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 Service 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 records with the Council's agreed provider for storing paper records can only be made through Business Support Unit. The provider will not accept requests directly from managers or other staff outside of Business Support Unit.

6.3.5 Some teams store records in storage rooms at the Civic Centre. In such cases, the Business Support Teams and/or Technical Administrative Teams in service areas are responsible for organising and managing the storage and retrieval of these records.

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, services must have in place clearly defined arrangements for the assessment and selection of records for disposal, and for documenting this work. Service 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 data must be destroyed in a secure way using confidential disposal facilities.

6.4.2 For paper records stored by the Council's agreed provider, the provider will destroy the records securely on behalf of the Council when the record reaches its designated destruction date (as requested by Technical Admin) 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, Service Managers will need to ensure that their teams are only retaining electronic records which are required. This includes electronic information held on shared drives, information published on the Council's intranet (Horizon) as well as email accounts.

6.4.5 For electronic case records, Service Managers will need local ICT system reports to monitor to identify which records need to be destroyed. Service Managers will need to work with the Corporate 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, and can be explained and referred to. 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 Head of Administrative, Licensing, Technical and Business Services manages the contract for the Council's off-site storage provider. Hillingdon Information Assurance Group 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; and

- Reviews of Council service's records.

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:

Muir Laurie, Senior Information Risk Owner (& Head of Business Assurance), **t:** 01895 556132, **e:** mlaurie@hillingdon.gov.uk

For further information about Data Protection, Freedom of Information and Records Management please contact:

Raj Alagh, Borough Solicitor and Statutory Data Protection Officer, **t:** 01895 250617, **e:** ralagh@hillingdon.gov.uk

For further information about the Council's off-site storage provider please contact:

Jill Covill, Head of Administrative, Licensing, Technical and Business Services, **t:** 01895 277418, **e:** jcovill@hillingdon.gov.uk

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 2021*.

Relevant Policies and Legislation

Relevant Council Policies

- Information Governance Policy;

- Data Protection Policy;

- Individual Rights Policy;

- Managing an Information Security Breach Policy;

- Lawful Basis for Processing of Personal Data Policy.

Relevant Standards and Legislation

- Public Records Act 1958 and 1967;

- Local Government Act 1972;

- Local Government (Access to Information) Act 1985;

- Freedom of Information Act 2000;

- 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 2018; and
    - Records Management Society of Great Britain Retention - Guidelines for Local Authorities 2003:1.

- General Data Protection Regulation (EU) 2016/679.

- Data Protection Act 2018.