HARINGEY COUNCIL

RECORDS RETENTION POLICY

PREPARED BY	Feedback & Information Governance Manager
AUTHORISED BY	Senior Leadership Team and Cabinet Member for Corporate Resources
DATE CREATED	13 March 2018
VERSION	1

REVISED	-
REVIEW DATE	09 March 2020

Contents

HARINGEY COUNCIL RECORDS RETENTION POLICY

1. Aim

1.1. This document sets out Haringey Council's approach to records retention and incorporates retention guidelines issued by the Local Government Association. The aim of this policy is to ensure best practice by:

- Assisting in identifying records that may be worth preserving permanently as part of a local authority's archives.
- Preventing the premature destruction of records that need to be retained for a specified period to satisfy legal, financial and other requirements of public administration.
- Providing consistency for the destruction of those records not required permanently after specified periods.
- Ensuring that the council does not retain information or records for longer than is necessary.

1.2. Proper retention and destruction of information is essential to assist the council achieving compliance of the Freedom of Information Act 2000 and Data Protection Act 2018.

1.3. This policy applies to all records held as recorded information by Haringey Council (in all formats, including paper, electronic, microform, audio-visual etc.), which are created, collected, processed, used, stored and/or disposed of by the authority's employees, partners and agents in the course of the authority's business activities.

2. Key roles and responsibilities

2.1. The information asset owner is responsible for ensuring that appropriate retention periods are identified for the records that they own and that processes are in place to ensure that records are destroyed appropriately in line with the retention period.

2.2. The information asset owner is the person responsible for delivering the function that the information is held in relation to and for making decisions on what information is held and how it will be used. This is usually the Head of Service or Assistant Director.

2.3. Haringey's record of Processing Activities captures details of all processing of personal information and identifies the information asset owner and appropriate retention period.

2.4. The Data Protection Officer is responsible for providing advice and guidance on the appropriate retention periods and destruction of records.

2.5. The Information Governance Board is responsible for monitoring the implementation of this policy. The Board is chaired by the Senior Information Risk Owner (SIRO) who has ownership of the organisation's information risk policy and information risk

management strategy. The Information Governance Board reports to the Council's Statutory Officers Group.

3. Background

3.1. Records are the Council's corporate memory and provide the evidence of the Council's business actions and decisions. They also provide evidence that the Council has satisfied statutory requirements. Well-managed records can improve the process of decision-making and facilitate business administration. They are, therefore, a corporate asset.

3.2. Any evidence of Council business activity is a record. Records, therefore, can be paper documents, electronic files, emails, databases, maps or images. The retention policy applies to all records irrespective of the format in which they are maintained or the media on which they are held.

3.3. The Council holds information for many purposes (e.g. service delivery, employment and business activities). Often, we must keep the information for a minimum number of years. The Council needs to know where all its information is, how long it should be kept and why it needs to be kept.

3.4. The Council's Retention Schedule is a 'living document' that will be amended and modified as and when retention details change or regulations and legislation that govern information and its use are introduced or changed.

3.5. The retention schedule is a tool to ensure best practice by:

- Assisting in identifying records that may be worth preserving permanently as part of a local authority's archives
- Preventing the premature destruction of records that need to be retained for a specified period to satisfy legal, financial and other requirements of public administration
- Providing consistency for the destruction of those records not required permanently after specified periods
- Ensuring that the council does not retain information or records for longer than is necessary

3.6. Proper retention and destruction of information is essential to assist the council achieving compliance with the Freedom of Information Act 2000, Environmental Information Regulations 2004, and Data Protection Act 2018 and the Local Government Act 1972.

4. Transfer of Records

4.1. This section relates to the transfer of records to off-site storage.

4.2. Many teams only retain paper records on site for a short period. Once the paper records are no longer in active use, they will be transferred to off-site storage. The records will then be retained for the periods outlined later in the retention schedule.

4.3. Where records are removed from the physical environment of the business unit into other physical areas whether directly controlled by the Council or by external third parties, the business unit (information asset owner) retains responsibility until disposal or transfer to archivist (historical/museum storage).

5. Destruction of Records

5.1. The destruction of records is an irreversible act. Many records contain sensitive and/or confidential information and must be destroyed in accordance with Council policy and, where possible, proof of secure destruction should be obtained.

5.2. Any records transferred to off-site storage must be destroyed by the relevant records company. The company should contact the relevant officer at the appropriate time and request confirmation that the records can be destroyed. A certificate of destruction must be provided.

5.3. Secure destruction of ICT equipment is carried out by Shared Digital.

5.4. The appropriate destruction method will depend on the classification of the record. Please refer to the How to Classify Information Policy for full guidance.

Official Classification

5.5. This is the default for Information that is created or processed by Haringey Council. This includes routine business operation and service information, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.

Official Sensitive

5.6. Official sensitive records or information would include those relating to:

- Commercial or market-sensitive information, including that subject to statutory or regulatory obligations that may be damaging to the Council or to a commercial partner if improperly accessed: and
- Particularly sensitive information relating to one or more identifiable individuals, where inappropriate access could have damaging consequences

	Official	**Official Sensitive**
Hardcopy	Should be shredded and securely disposed or placed in secure confidential waste bins	Must be shredded and securely disposed or placed in secure confidential waste bins
Electronic	Should be deleted by users from the Council's network when the information has reached its lawful or regulatory retention period	Should be deleted by users from the Council's network when the information has reached its lawful or regulatory retention period.

5.7. For further guidance, refer to the Information Handling, Labelling and Disposal Procedure.

6. Retention Schedule

6.1. The Council undertakes to have due regard to the LGA Records Retention Guidance in setting appropriate retention periods for the personal data it holds. The Council will maintain links on its own Information Governance intranet pages and through its guidance to officers will direct officers to maintain their awareness of that guidance.

6.2. All records created or received by the Council must be assigned a retention period in line with that guidance, unless there is a business reason for deviation.

6.3. If the guidance does not cover the particular processing activity, officers must approach the Data Protection Officer for advice on determining an appropriate retention schedule.

6.4. If there is a business reason for deviating from the LGA guidance, this should be approved by the Data Protection Officer and captured in the record of Processing Activities.

6.5. A retention period is based on two factors, an event and a time period. An event may be the record's creation date; record's closure date; a calendar event such as the end of a financial year or an external event such as a contract end date. The time period can vary from months to permanent retention. At the end of the retention period the records must be destroyed.

6.6. Unless the guidance specifies otherwise, personal data must not be held for longer than 6 years after the data subject's last contact with the Council. This period reflects the general time within which, under the Limitation Act 1980, a civil action could be brought before the courts. It should also be noted that, under this Act, civil action could be taken up to twelve years following certain events.

6.7. Exceptions to the six-year period may occur when records:

- are held in legal documents 'under seal' where they may have to be retained for up to twelve years
- need to be retained because the information contained in them is relevant to legal action which has been started
- are required to be kept for longer or shorter period by statute
- are archived for historical purposes

6.8. Records that have no significant operational, informational or evidential value should be destroyed as soon as they have served their primary purpose. These might include:

- Announcements and notices of meetings and other events, and notifications of acceptance or apologies

- Requests for, and confirmations of, reservations for internal services (e.g. meeting rooms) where no internal charges are made
- Superseded address lists and distribution lists
- Personal diaries, address books etc.
- Working papers, where the results have been written into an official document and which are not required to support it

7. Approval & Review

7.1. This policy has been approved by the Cabinet Member for Corporate Resources.

7.2. The policy will be reviewed by The Data Protection Officer and Information Governance Board biennially or on an exception basis if there are any changes to the relevant legislation and guidance, any applicable audit recommendations or any other reason to review or amend the policy.

8. Relevant polices and procedures

8.1. This policy should be read in conjunction with Haringey's Data Protection Policy.