NOTICE OF MEETING

CABINET MEMBER SIGNING

Friday, 6th April, 2018, 2.00 pm - Civic Centre, High Road, Wood Green, N22 8LE

Councillor Ali Demirci – Cabinet Member for Corporate Resources

Quorum: 1

1. FILMING AT MEETINGS

Please note that this meeting may be filmed or recorded by the Council for live or subsequent broadcast via the Council's internet site or by anyone attending the meeting using any communication method. Although we ask members of the public recording, filming or reporting on the meeting not to include the public seating areas, members of the public attending the meeting should be aware that we cannot guarantee that they will not be filmed or recorded by others attending the meeting. Members of the public participating in the meeting (e.g. making deputations, asking questions, making oral protests) should be aware that they are likely to be filmed, recorded or reported on.

By entering the meeting room and using the public seating area, you are consenting to being filmed and to the possible use of those images and sound recordings.

The chair of the meeting has the discretion to terminate or suspend filming or recording, if in his or her opinion continuation of the filming, recording or reporting would disrupt or prejudice the proceedings, infringe the rights of any individual or may lead to the breach of a legal obligation by the Council.

2. URGENT BUSINESS

The Leader/Cabinet Member will advise of any items they have decided to take as urgent business.

3. DECLARATIONS OF INTEREST

A member with a disclosable pecuniary interest or a prejudicial interest in a matter who attends a meeting of the authority at which the matter is considered:

(i) must disclose the interest at the start of the meeting or when the interest becomes apparent, and

(ii) may not participate in any discussion or vote on the matter and must withdraw from the meeting room.

A member who discloses at a meeting a disclosable pecuniary interest which is not registered in the Register of Members' Interests or the subject of a pending notification must notify the Monitoring Officer of the interest within 28 days of the disclosure.

Disclosable pecuniary interests, personal interests and prejudicial interests are defined at Paragraphs 5-7 and Appendix A of the Members' Code of Conduct

4. DATA PROTECTION POLICY AND DATA RETENTION POLICY UPDATES NON KEY (PAGES 1 - 20)

5. URGENT BUSINESS

As per item 2.

Ayshe Simsek
Committees Manager
Tel –0208 4892929
Fax – 020 8881 5218
Email: philip.slawther@haringey.gov.uk

Bernie Ryan
Assistant Director – Corporate Governance and Monitoring Officer
River Park House, 225 High Road, Wood Green, N22 8HQ

Tuesday, 27 March 2018

Agenda Item 4

Report for: **Non Key Cabinet Member Signing**

Title: Updated Data Protection and Records Retention Policies

Report authorised by : Richard Grice – Interim Director for Transformation and Resources

Lead Officer: Anita Hunt, 1844, anita.hunt@haringey.gov.uk

Ward(s) affected: N/A

Report for Key/ Non Key Decision: Non key decision

1. Describe the issue under consideration

1.1 New Data Protection legislation will come into force on 25 May 2018. This significantly increases the maximum level of fine that can be applied in respect of breaches of the legislation (from £500,000 up to £17 million). The data protection and records retention policies have been reviewed and updated to refer to and ensure compliance with the new legislative requirements. The Cabinet Member for Corporate Resources is asked to approve these policies.

1.2 The safety and integrity of personal data is a matter of great importance to the public. The Data Protiection policy sets out our statement of intent in ensuring we work to the high standards our residents and customers would expect.

1.3 With regards to the Records Retention Policy, the policy states the Council will adopt the Local Government Association (LGA) guidance to inform its own retention schedule. The ensures Haringey is closely aligned to recognised good practice within local government.

2 Cabinet Member Introduction

N/A

3 Recommendations

3.1.1 That the Cabinet Member approves the Data Protectionpolicy attached at appendix 1 and further approves Records Retention policies attached at appendix 2.

4 Reasons for decision

4.1 To ensure that these key policies are up-to-date, reflect the new legislation and are in force when the legislation comes into force on 25 May 2018.

5 Alternative options considered

The Council is legally required to update these policies in line with legislation.

6 Background information

6.1 The change in legislation requires us to update the policies. In addition, a recent internal audit report into Information Governance – Information Retention recommended:

> *An Information Retention policy should be developed that incorporates new legislation and current practices. The document should be formally approved and disseminated to staff.*

6.2 It is essential that these key policies are in place (along with the supporting procedural documents for the Data Protection Policy) when the new legislation comes in to force.

7 Contribution to strategic outcomes

7.1 These policies support the Council's strategic outcomes by providing a basis for efficient and compliant information management across all council functions.

8 Statutory Officers comments (Chief Finance Officer (including procurement), Assistant Director of Corporate Governance, Equalities)

Finance

8.1 Owing to the requirement to address the statutory changes where the financial risk of non-compliance has risen from a £500k penalty to £17m, compliance to the new statute is pararmount.

8.2 The Records Rention policy will formally adopt the practices already in place and will created no additional financial burden.

8.3 It should be noted that adherence to the data protection policy may mean a need to increase the resources devoted to Information Governance to support and demonstrate our compliance with the new legislation. This report is only considering a formal adopting of the policy and if additional resources are required, that will form the basis of a report at a later date.

Procurement comments

8.4 The Head of Procurement notes the contents of this report and concurs with the recommendation

Legal comments

8.5 The Assistant Director Corporate Governance has been consulted in the preparation of this report and makes the following comments. He sees no legal reason why the recommended decision should not be made.

8.6 The General Data Protection Regulation (the GDPR), which makes significant changes to data protection law throughout the EU, takes effect on 25 May 2018. In particular, for the Council, it introduces a new basis for data processing ("public task") but restricts reliance on the existing bases of consent and legitimate interest. It also requires the basis/bases upon which data is processed to be identified from the beginning, rather than after the event; and that this be communicated upfront to the individual whose data is being processed.

8.7 The Data Protection Bill (the Bill), which reaches Committee stage in the House of Comons on 13 March 2018, is expected to become law and be brought into force to coincide with the GDPR. When it becomes law, it will repeal the Data Protection Act 1998, which is the current basis of data protection law.

8.8 As relevant to the Council, the Bill:

- addresses areas within the GDPR that are left to the discretion of the UK
- extends data processing law into types of processing not covered by the GDPR
- provides a single regime for data processing for law enforcement purposes (in so doing transposing the Law Enforcement Directive into UK law)
- introduces new powers and offences in relation to data protection

8.9 These legislative changes require updating of the Council's policies to ensure compliance.

Equality Comments

8.10 The Council has a Public Sector Equality Duty under the Equality Act (2010) to have due regard to the need to:

- Eliminate discrimination, harassment and victimisation and any other conduct prohibited under the Act
- Advance equality of opportunity between people who share those protected characteristics and people who do not
- Foster good relations between people who share those characteristics and people who do not

8.11 The report details amendments to the Council's existing Data Protection and Retention policies, as a result of national legislative changes. These changes are not expected to impact negatively on protected groups.

8.12 Overall, the changes will require the Council to be more transparent in its use of personal data. In addition, certain categories of information such as race and ethnicity, religious beliefs and sexual orientation will receive further protection to ensure that the security of personal information is maximised.

8.13 The Council will continue to consider potential impacts and comply with existing equality obligations as part of the application of the new Data Protection and Retention policies.

9 Use of Appendices

Appendix 1: Data Protection Policy
Appendix 2: Records Retention Policy

10 Local Government (Access to Information) Act 1985
None

HARINGEY COUNCIL
DATA PROTECTION 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

DATA PROTECTION POLICY

1. Introduction

1.1. The council collects, holds and processes lots of information including personal information about the people it serves, including local residents and businesses, and its employees.

1.2. The Data Protection Act 2018 (the Act) is, with the General Data Protection Regulations (GDPR), the legal framework that ensures personal information relating to living individuals is handled properly and gives individuals rights in relation to their personal information, such as to access the information that is held about them.

1.3. This Policy sets out how Haringey Council will comply with the Act. It should be read in conjunction with Shared Digital IT Security policies which set out the technical measures in place to ensure that information on our IT systems is held securely and the measures to ensure privacy by design and default in procurement and development of our IT systems.

2. Policy statement

2.1. The Council is fully recognizes its responsibilities to act as responsibly in how personal information is handled and to upholding the rights of individuals in respect of that information. As such it supports and is committed to uphold the following principles:

- Personal data shall be processed lawfully, fairly and in a transparent manner
- Personal data will only be collected for a specified, explicit and legitimate purpose and will not further processed or archived in a manner that is incompatible with those purposes;
- The Council will ensure we collect and process data that is adequate, relevant and limited to what is necessary in relation to the purposes
- The Council will keep data accurate and up-to-date, and correct or delete inaccuracies in a timely manner
- Personal data will not be kept in a personally identifiable form for longer than necessary for the purpose; and if stored for longer periods for archiving in public interest, research or statistical purposes will be subject to appropriate technical and organisational measures to safeguard the rights and freedoms of people;
- The Council will ensure through technical and organizational measures, the security and integrity of the personal data it holds, against unauthorized or illegal processing, accident loss, destruction or damage.

3. Aim

3.1. This policy aims to ensure that:

- procedures are in place to ensure the Council complies with its legal responsibilities in relation to the Act
- all officers understand and undertake their responsibilities in relation to the Act
- compliance with this Policy is monitored and the Council is able to evidence that it is complying with its legal responsibilities.

3.2. This Policy applies to all employees, contractors, consultants, agency staff and other users of Haringey Council's information. The Policy is also applicable to elected Members who create and use records in their capacity as representative of the Council.

3.3. The Policy applies to all personal information created, received, stored, used and disposed of by the Council irrespective of where or how it is held.

4. Key roles and responsibilities

4.1. **All officers** whose role involves access to personal information held by Haringey council are responsible for compliance with this policy, for handling information in accordance with our IT Security policies and for following the processes and guidance that support these policies. It is a breach of Haringey's Staff Code of Conduct to misuse personal information; misuse could result in disciplinary action or dismissal.

4.2. **Managers** must ensure that their staff are aware of and adhere to this policy and the data protection requirements within their area of work. They must disseminate any associated procedures and guidance to their staff and ensure that they have completed the data protection training.

4.3. **Information asset owners** are 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. Information Asset owners must ensure that their processing activities are compliant, properly documented in the Record of Processing Activities and that consideration of privacy and data protection is integral to any consideration of new policies, business processes, projects and contracts.

4.4. The Data Protection Officer's (DPO) key responsibilities will be:

- To inform and advise the organisation and its employees about their obligations to comply with the Act and other data protection laws.

- To monitor compliance with the Act and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.

- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

4.5. **The Senior Information Risk Owner (SIRO)** has ownership of the organisation's information risk policy and information risk management strategy.

4.6. **The Caldicott Guardian** is the senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly.

4.7. **The Information Governance Board** is responsible for overseeing and leading the work of council Departments in relation to Information Governance and to ensure compliance with relevant statutory and local requirements, taking account of industry standards/recognised best practice. The Board will be chaired by the SIRO.

5. Documenting our processing activities

5.1. We will keep and maintain a Record of Processing Activities (ROPA) for all council functions that involve handling personal information. The ROPA will include the following:

- The purposes of the processing
- The appropriate legal basis for processing (as contained in the Act)
- Who processes the information (council officers or others on our behalf according to our instruction)
- The location of the information
- Security measures
- The different types of people whose personal data is processed,
- the categories of personal data we process
- The recipients of personal data
- Whether we use the information to make automated decisions or conduct profiling of the information subject
- How long the information is kept

5.2. The ROPA will be compiled, held and monitored by the Data Protection Officer and made available on request to members of the public, partners and the Information Commissioner's Office.

6. Privacy Notices

6.1. We will inform the people whose personal data we process how and why we process their information by providing appropriate privacy notices when we obtain their data.

7. Consent

7.1. Where we rely on consent as the legal basis for our data processing activities, we will ensure that genuine and explicit consent is obtained and that we are able to demonstrate that.

8. Special Category Information

8.1. The Act applies additional safeguards to information relating to: race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation (referred to in the Act as “special category” data).

8.2. The Council will not hold special category information unless it is necessary to do so. Where special category information is held, Haringey Council will ensure that one of the necessary conditions at Schedule 1 of the Act is met and that this is supported by an appropriate policy document, where applicable.

9. Individual Rights

9.1. The Council will uphold the following rights as enshrined in the Act:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

9.2. The Data Protection Officer will ensure that appropriate procedures are in place to enable people to exercise their data protection rights in compliance with the Act.

10. Training

10.1. All officers that handle personal information must complete the Data Protection and IT Security e-learning courses. This forms part of our corporate induction for new employees. Existing employees must retake the course annually; compliance will be monitored by the Data Protection Officer and Information Governance Board.

10.2. Staff will have access to up-to-date policies, procedures, guidance and training through the intranet.

11. Privacy by design and default

11.1. We will institute organisational measures to ensure that data protection and privacy issues are incorporated into our consideration of new policies, business processes and projects. These will include:

- Our project management framework Organisation Impact Assessment to address data protection considerations.

- Our formal decision-making processes to include data protection considerations.

- Privacy Impact Assessments to be completed when using new technologies or where the proposed processing is likely to result in a high risk to the rights and freedoms of individuals.

11.2. Our Shared Digital IT service will ensure that appropriate technical measures are taken to ensure privacy by design and default in procurement and development of our IT systems.

12. Personal data security breaches

12.1. We will record all personal data security breaches and report them to the Information Commissioner's Office as required by the Act in accordance with our Personal Data Security Breach Procedure. Details of security breaches will be reported to the Information Governance Board quarterly.

13. Contracts with processors

13.1. We will ensure that we have written contracts with all people or organisations that process personal information on our behalf so that both parties understand their data protection responsibilities and liabilities.

14. Approval & Review

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

14.2. 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.

15. Relevant polices and procedures

15.1. This policy should be read in conjunction with Haringey's IT Security Policy and
15.2. Records Retention policy.

15.3. The following procedures support this policy and provide detailed guidance for compliance:

- Personal Data Security Breach procedure
- Individual Data Protection Rights Procedure (includes subject access)
- Use of Personal Data for a Different Purpose Assessment Procedure
- Privacy Impact Assessment process and forms

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.