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	1.3
REVISED	20 January 2023
REVIEW DATE	20 January 2025

DOCUMENT HISTORY			
DATE	**ISSUE**	**SECTION**	**REVISION DETAILS**
13/03/18	1.0	All	First draft
19/07/21	1.1	All	Reviewed, amended by DPO, approved by IG board 12/10/21
20/01/23	1.2	All	Reviewed, amended by DPO, approved by IG board 21/02/23

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 UK GDPR (General Data Protection Regulations) and EU 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 Digital Services' 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 fully recognises its responsibilities to act responsibly in how personal information is handled and to uphold 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 can 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 as defined in Article 39 of the UK GDPR are:

- to inform and advise the Council and our employees of our obligations to comply with the UK GDPR and other data protection laws;
- to monitor compliance with the UK GDPR and other data protection laws, and our data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
- to advise on, and to monitor Data Protection Impact Assessments (DPIA)
- to cooperate with the ICO; and to be the first point of contact for the ICO and for individuals whose data is processed (employees, customers etc).

- When carrying out their tasks the DPO is required to take into account the risk associated with the processing the Council is undertaking. The DPO must have regard to the nature, scope, context, and purposes of the processing.
- The DPO should prioritise and focus on the riskier activities, for example where special category data is being processed, or where the potential impact on individuals could be damaging. Therefore, DPOs should provide risk-based advice to the Council.
- If the Council decides not to follow the advice given of the DPO, the reasons should be documents to help demonstrate our accountability.

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. National Data opt-out for Health and Care Data

10.1 A system of opt-out for use of health and care personal data (including pseudonymised data) has been implemented by the NHS. We are required to comply with this. We will therefore:

- Ensure that all data extracts for non-direct care purposes are filtered to remove patients who have opted out
- Ensure that we make patients aware of their rights.
- Where data is being manually extracted for non-care purposes, we will ensure that records are manually checked for opt-out

11. Training

11.1. 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.

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

12. Privacy by design and default

12.1. 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.

12.2. Our Digital Services will ensure that appropriate technical measures are taken to ensure

privacy by design and default in procurement and development of our IT systems.

13. Personal data security breaches

13.1. 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.

14. Contracts with processors

14.1. 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.

15. Approval & Review

15.1. This policy has been approved by the Cabinet Member for Finance and Local Investment.

15.2. 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.

16. Relevant polices and procedures

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

16.3. 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)
- Privacy Impact Assessment process and forms