Data Protection Policy

Version 2.0, February 2024

Revision history

Date	Version	Summary of action	Author
May – June 2012	0.1 – 0.6	Policy creation	Sinead Mulready
September 2012	1.0	Published policy	Sinead Mulready
June 2014	1.1	Annual policy review	Sinead Mulready
February 2017	1.2	Review and update of roles	Shona Nicolson
March 2018	1.3	Annual policy review and preparation for GDPR	Leila Ridley
May 2019	1.4	Annual policy review	Antoinette Carter
December 2020	1.5	Annual review: converted to accessible format and updated to UK GDPR	Leila Ridley
December 2021	1.6	Annual policy review	Leila Ridley
December 2022	1.6	Annual policy review	Leila Ridley
December 2023	1.7	Updated as part of policy framework review	Leila Ridley
February 2024	2.0	Published	Leila Ridley

Table of Contents

1. Purpose of this document

This document sets out the policy under which the council processes personal data and forms part of the council's Information Governance Policy Framework. The policy aims to ensure that Islington Council complies with its obligations under data protection. This policy must be read in conjunction with the council's cyber security and acceptable use policies.

This policy is applicable to council employees, councillors, temporary and agency staff and contractors working for and on behalf of the council and any organisations processing data on the council's behalf.

2. What is personal data?

For data to be personal, it must relate to a living individual, and not, for example, a company or a deceased person. If information can identify a living individual, it is the personal data of that individual. The definition of personal data within the Data Protection Act 2018/UK General Data Protection Regulation is:

"Personal data means any information relating to an identified or identifiable living individual. Identifiable living individual means a living individual who can be identified, directly or indirectly, in particular by reference to:

a) *an identifier such as a name, an identification number, location data or an online identifier, or*

b) *one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual."*

3. Background

The council needs to collect and use certain types of information about its staff, residents, customers and clients to carry out its functions. Personal information must be obtained, held, used or disclosed appropriately whether it is recorded on paper, stored in a computer database, or recorded on other material. The council must process such information in accordance with the requirements of the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (UK GDPR).

The council is committed, to processing personal data according to legislation and best practice guidelines as recommended by the Information Commissioner's Office (ICO). The ICO is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Further information about the Data Protection Act and the UK GDPR is available from the Information Commissioner's Office, at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Telephone: 0303 123 1113.

Alternatively, visit Contact us | ICO

4. Applying the policy

4.1 The council must be a registered Data Controller

The council makes decisions about how personal data are processed, which means it must notify this processing to the ICO (unless an exemption applies) and register as a Data Controller. UK GDPR defines a data controller as a (legal) person, who determines the purposes and means of the processing of personal data. It is responsible for notifying the ICO with a description of the personal data being (or to be) processed, and the purposes for which the data are being (or are to be) processed. The council is the registered Data Controller.

Members of the Senior Leadership Team have been appointed as Information Asset Owners (IAOs) and they are responsible for informing the Data Protection Officer of any new purposes for which personal data are processed to ensure the council's notification is kept up to date.

The registration number for the council is Z6018243

4.2 The council will appoint a Data Protection Officer

The council must appoint a Data Protection Officer (DPO). This is a mandatory role and defined by Article 39 of UK GDPR. The role provides independent advice to the council and can report directly into CMT when required. The minimum tasks, as defined by UK GDPR, are:

- To inform and advise the organisation and its employees about their obligations to comply with the UK GDPR and other data protection laws.
- To monitor compliance with the UK GDPR 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 (residents, employees, customers etc.).

4.3 The council must process personal data in accordance with the law

Article 5(1) of the UK GDPR sets out seven principles that are at the heart of the regime. The council must comply with these principles when processing personal information. The principles are:

a) Processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’).

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered incompatible with the initial purpose (‘purpose limitation’).

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’).

d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’).

e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation').

f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Article 5(2) of UK GDPR adds:

- The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability'). Take responsibility for what the council does with personal data and how we comply with other principles. The council will have appropriate measures and records in place to demonstrate compliance (accountability).

Complying with these principles is essential for good data protection practices and failure to comply with them can result in regulatory action, including monetary penalties by the ICO.

4.4 The council must have a lawful basis to process data

To comply with the principles, the council must have a lawful basis to process personal data, this means that we must have a specific reason to collect, use and store personal information. There are six lawful bases in UK GDPR and the council must chose the most appropriate basis, this must be identified before the information is processed.

If the council is processing special category data (sensitive personal data) then it must identify a lawful basis for general processing and an additional condition for processing this more sensitive information.

If the council is unable to identify a lawful bases to process the information, then it cannot process the information. The ICO have produced a helpful guide on lawful bases: A guide to lawful basis | ICO

4.5 The council will have privacy notices

The council must be transparent with individuals regarding the data being processed and we must inform people when we are processing their information. This information is contained in a privacy notice and must ensure that individuals:

- Understand what data is being processed (including the legal basis for this processing).
- Who we share their data with (both within and outside the council).
- How long we will keep their information for.
- Their right to complain to the ICO and how do to this.

This is known as ‘the right to be informed’. The UK GDPR is explicit in what must be included in the privacy notice and to ensure that we are compliant, the council has adopted a layered privacy notice approach. The council has a corporate privacy notice on its website and from here, individuals can access service specific privacy notices.

All Service Directorate Level Notices must be reviewed by the Information Governance Team and in some cases be reviewed by Legal Services before they are published.

4.6 The council will have good accountability and governance

4.6.1Contracts and data sharing

The council will only share data where it has a clear lawful basis to do so and will ensure that all data sharing is justified.

Where the council commissions a third party to carry out a service (or process data) on our behalf a contract must be in place. This contract must have appropriate data protection clauses and include a data protection schedule clearly identifying what data will be shared. The council will ensure that contract due diligence and effective monitoring takes place on all contracts involving personal data.

The council will have clear processes in place where it routinely shares personal data with another council department or a third-party organisation. Where appropriate Data Sharing Agreements (DSAs) will be in place. All sharing agreements will comply with the ICO’s Code of Practice on data sharing.

4.6.2The council will maintain documentation

The council will document its processing activities in line with its article 30, UK GDPR obligations. The council will maintain a comprehensive Record of Processing Activities (ROPA) and Information Asset Register (IAR) and develop clear data flow maps to ensure there is good governance of data flows. Details of how the council manages this work can be found in the Records Management Policy and Information Asset Owner procedure.

4.6.3The council will have data protection by design and default

The council will consider data protection and data privacy issues upfront. To comply with article 25 of the UK GDPR the council will ensure that it only processes data that is necessary to achieve the specific purpose. The council will consider the following in all its processing:

- Adopting a ‘privacy-first’ approach with any default settings of systems and applications.
- Ensuring that it is clear to individuals when they have true choice over the information we process.
- Only process additional data where there is a clear lawful basis to do so, this includes further processing.

- Ensuring that personal data is protected and is only made publicly available if the individual decides to make it so.
- Providing individuals with sufficient controls and options to exercise their rights.
- Restrict the use of generative AI where appropriate.

4.6.4 The council will carry out data protection impact assessments

The council will conduct data protection impact assessment (DPIA) screening on all projects that involve the processing of personal data, including those involving new technology. Where processing is likely to result in a high risk to the rights and freedoms of individuals the council will carry out DPIAs to ensure that all risks are fully explored.

Details of the council's approach to managing DPIAs is set out in the council's Data Protection Procedures.

4.6.5Pseudonymisation and anonymisation

Where the council wishes to use personal data for secondary purposes, it shall ensure that the data is pseudonymised or anonymised.

Secondary use refers to the use of information about individuals where their personal data is used for purposes that do not directly contribute to the safe care of the person concerned. When Personal Identifiable Information (PID) is required for secondary use, it should be limited and de-identified so that the person's confidentiality is not compromised. This could be for:

- Research purposes
- Capacity planning and commissioning
- Contract monitoring
- Service Redesign and benchmarking
- Audits and reporting facilities

'Pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

The aim of 'anonymisation' to obscure the identifiable information items within the person's records sufficiently so that the risk of potential identification is minimised.

Details of how pseudonymisation and anonymisation can be applied is set out in guidance that can be found on Islington Connect.

4.7 The council will facilitate all individual's rights

The council is committed to being open and transparent the council will maintain an Access to Information Policy which will describe the arrangements and practices that are in place to ensure that the council can respond appropriately to any request made in relation to Individual's Rights; and to provide clarity on the way in which the council will meet its duties under the DPA and UK GDPR, guidance and best practice. The council will ensure that details of how to make a request are clearly set out on the council's website Individuals' rights | Islington Council.

4.8 The council will ensure that personal data are accurate

The council will ensure that personal data are accurate. The council will ensure, where reasonably possible, that personal information is kept up to date and will take steps to update its systems when informed that data needs to be updated. The council will investigate any complaint that relates to data accuracy, including where data has not been updated in a timely manner.

4.9 The council must store data securely

The council ensures appropriate technical and organisational measures against unauthorised processing of personal data; unlawful processing of personal data; and accidental loss or destruction of, or damage to, personal data. Information and records relating to service users will be stored securely and will only be accessible to authorised and trained staff and volunteers.

The council has an ICT Policy Framework, consisting of the council's security standards, including the use of passwords, encryption and anti-virus software.

4.10 Data Breaches

The council has a duty to ensure that all personal data that it processes is kept secure. To manage the risk of data breaches, the council has robust breach detection, investigation and internal reporting procedures in place.

The council will ensure that where breaches are deemed to result in a high risk to, or adversely affect, the rights and freedoms of individuals clear processes are in place for the IDG team to assess and report the matter to the ICO within 72 hours and that individuals are informed without undue delay.

Full details of the council's approach can be found in the Data Breach Policy.

4.11 The council must ensure that staff understand their responsibilities

The council recognises that to support compliance with our obligations it is essential that all staff are trained to understand their obligations in relation to protecting data, including, data handling, security and appropriate information governance protecting data and the Information and Digital Governance (IDG) team will ensure that there is an ongoing mechanism for maintaining good awareness of information governance matters.

The council will use a variety of methods to promote council awareness:

- A training approach that clearly sets out all mandatory training, including eLearning delivered via pop up functionality to computer users and 'classroom' training for staff without routine access to the council's network.
- Ensuring that policy and general information is available on the council's intranet.
- Using corporate communications channels for targeted messages.
- Attending Departmental Management Team meetings to raise specific issues.

The council will also ensure that:

- Staff processing personal information understand that they are responsible for complying with the data protection principles.
- Staff processing personal information are appropriately trained to do so.
- Staff processing personal information are appropriately supervised.
- Staff with enquiries about handling personal information know who to ask.
- Enquiries about handling personal information are dealt with promptly and courteously.
- It describes clearly how it processes personal information.
- It regularly reviews and audits the ways it obtains, holds, uses or discloses personal information.
- It regularly assesses and evaluates its methods and performance in relation to handling personal information.
- All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them.

For further information about Islington Council's compliance with data protection law, please contact us: dp@islington.gov.uk