ISLINGTON

Islington Data Protection Policy

A council-wide information policy
Version 1.3
March 2018

Contacts

If you need any further information about this document or any clarity about the contents of the document, please contact: The Information Governance Team (foia@islington.gov.uk).

Revision History

Date	Version	Reason for change	Author
13 May 2012	0.1	First draft	Sinead Mulready
6 June 2012	0.2	Reviewed by Peter Fehler	Sinead Mulready
6 June 2012	0.3	Reviewed by Jeremy Tuck	Sinead Mulready
12 June 2012	0.4	Reviewed by Robin Ingram (Hytec)	Sinead Mulready
20 June 2012	0.5	Reviewed by Jeremy Tuck	Sinead Mulready
02 August 2012	0.6	Changes incorporated following CAB and DSWG consultation review	Jeremy Tuck
September 2012	1.0	Approved by Audit Committee and published on website	Sinead Mulready
June 2014	1.1	Annual review	Sinead Mulready
Feb 2017	1.2	Review and update of roles	Shona Nicolson
March 2018	1.3	Annual review	Leila Ridley

Distribution:

This document has been distributed to:

Name	Role
Peter Fehler	Service Director Corporate and Dispute Resolution
Corporate Governance Group and Data Security Working Group	Boards and groups responsible for corporate data protection and setting data protection policy
All staff	For action

TABLE OF CONTENTS

1 PURPOSE OF THIS DOCUMENT

This document sets out the policy under which Islington Council processes personal data. The policy is applicable to Islington Council employees, agency staff, volunteers, contractors, services providers and other organisations or agencies working for or on behalf of the council.

2 WHAT IS PERSONAL DATA?

In order 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/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 in order 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 General Data Protection Regulation (GDPR).

The council is committed, to processing personal data according to legislation and best practice guidelines as recommended by the Information Commissioner's Office. The Information Commissioner's Office 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 General Data Protection Regulation is available from the Information Commissioner's Office, at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Telephone: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate.

Alternatively, visit www.ico.org.uk or email casework@ico.org.uk.

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 Information Commissioner's Office (unless an exemption applies) and register as a Data Controller. 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 Information Commissioner 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.

Heads of Service 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 in order 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. This is a mandatory role and defined by Article 39 of the GDPR. The role provides independent advice to the council and is able to report directly into CMB when required. The minimum tasks, as defined by GDPR, are:

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

The council will comply with the six Data Protection Principles as set out in the GDPR/DPA in relation to personal data that the council processes, that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').
- 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, in accordance with Article 89(1), not be considered incompatible with the initial purpose ('purpose limitation').
- Adequate, relevant and not limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').
- 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').
- 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 in accordance with Article 89(1) 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').
- 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').

4.4 The council will have a Privacy Notice

The GDPR sets out an obligation on data controllers to ensure that the individuals whose data it is processing understand what data is being processed (including the legal basis for this processing), who the council is sharing it with (both within and outside the organisation), how long we will keep it for and their right to complain to the Information Commissioner's Office (ICO). This is known as 'the right to be informed'. The 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 will be able to access service specific privacy notices.

Where a directorate has a requirement to use alternative wording, the proposed wording must be reviewed by the Information Governance Team and Legal Services.

4.5 The council will facilitate all the Individual's Rights

The council will maintain an Individual's Rights Handling Procedure which will describe 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 Data Protection Act and the General Data Protection Regulation, guidance and best practice.

4.6 The council must 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. The council will investigate any complaint that relates to data accuracy.

4.7 The council must store data securely

The council takes 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 policies that describe how data is stored and accessed by employees, along with the council's security standards, including the use of passwords, encryption and anti-virus software. These policies are available on the council website.

4.8 The council must ensure that staff understand their responsibilities

The council will ensure that:

- It has a Data Protection Officer with specific responsibility for ensuring compliance with the Data Protection Act/General Data Protection Regulation;
- 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; and
- 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.

4.9 Information Sharing Agreements

Where the council routinely shares personal data with a third party, an Information Sharing Agreement will be put in place.

An Information Sharing Agreement (ISA) is a written agreement between two or more organisations to routinely share personally identifiable data. The council must use a contract when we commission a third party to carry out a service (or process data) on our behalf. An Information Sharing Agreement should be used when two organisations have a statutory right or duty to share data in order to each deliver their own services.

If we share council data with a third party and do not set out the legal justification, the arrangements and responsibilities, we will be legally responsible for anything that happens to that data, or anything the third party does. They could:

1. Lose the data
2. Publish it online
3. Mis-use it (email marketing information or spam to our residents)
4. Allow a member of their staff to access it maliciously, or sell it
5. Keep the data indefinitely.

4.9.1 Guidance on Information Sharing Agreements

1. The council officer who owns the ISA must identify the relevant staff in the other organisation(s) that data is to be shared with, and work with them to establish what data will be shared and how this will happen (ie, what systems will be used, who might have access, how regularly sharing will take place, and when the arrangement will be reviewed).
2. The ISA will be reviewed by the Information Governance Team and Legal Services at council's Information Governance Review Panel.
3. The council's Senior Information Risk Owner will sign on behalf of the council.
4. Send a final copy to the IG Team who will hold a register of all ISAs.

4.10 Management and reporting of ISAs

The Information Governance Team will hold a central register of all Information Sharing Agreements. This will include:

- The title
- A brief description of the sharing
- The signatories (ie the organisations that it covers)
- The owner (member of LBI staff with responsibility for maintaining the ISA)
- The date when it is subject to review.

The Information Governance Team will email the relevant owner when an ISA is within six months of its review date.

ISAs will be managed by exception – a list of any out of date ISAs will be brought to CGG as an information risk.

5 ROLES AND RESPONSIBILITES

5.1 Overview

This section describes the roles and governance arrangements in place to ensure that the council meets its requirements under the Data Protection Act 2018 and the General Data Protection Regulation.

5.2 Corporate Management Board will receive reports on Data Protection and security

The Corporate Management Board will receive reports that relate to information governance and data security as appropriate. These will be presented by the chair of the Corporate Governance Group, who will also serve as the council's Senior Information Risk Owner.

5.3 The Corporate Governance Group will receive reports on data protection and security

The Corporate Governance Group will receive reports on improved data assurance, records management processes and will monitor risks relating to data security issues. Reports will be submitted by the Information Governance Team, who has the remit for corporate information compliance.

5.4 The Information Governance team will raise risks as appropriate

The Information Governance Team will raise risks related to data security and report these as appropriate:

a) The Head of Information Governance & Business Support will determine when risks should be escalated to the Corporate Governance Group and the Corporate Risk Manager and will prepare reports for this board when necessary.

b) The Data Protection Officer will respond (reactively) to data security incidents as they arise and manage a process of improvement (proactively) through the Data Security Working Group. The Data Protection Officer will highlight risks to the Senior Information Risk Owner.

c) The Information Compliance Manager is corporately responsible for managing the council's approach to access to information requests and ensures that these are processed these according to the council's responsibilities for records management. The Information Compliance Manager will provide assurance by chairing an Information Governance Officer's meeting at least four times a year, where matters will be raised and risks discussed. Any matters that need to be escalated will be highlighted to the Senior Information Risk Owner. The Information Compliance Manager will provide reports on the council's compliance with access to information requests and these will be submitted regularly to the Corporate Management Board and Corporate Governance Group.

d) The Access to Information Manager has day-to-day responsibility for ensuring that the council effectively manages and responds to access to information requests. The Access to Information manager will facilitate a quarterly Information Governance Officer meeting and act as the main reference point on all matters relating to access to information. The Access to Information Manager will provide reports on the council's compliance when dealing with access to information requests.

5.5 Service areas must be represented at Information Governance Officer Meetings

Service areas must ensure that there is appropriate representation at the council's Information

Governance Officer meetings and will raise issues related to information management, records management and access to information where appropriate. Any issues raised at these meetings will be escalated by the chair of the meeting, the Information Compliance Manager, who will raise these matters with the Senior Information Risk Owner where necessary.

5.6 Service areas must be represented at the Data Security Working Group

Service areas must ensure that there is appropriate representation at the council's Data Security Working Group and will raise issues related to data security, data breaches and security policy where appropriate. Any issues raised at these meetings will be escalated by the chair of the meeting, the Data Protection Officer, who will raise these matters with the Senior Information Risk Owner where necessary.

5.7 All staff must be trained on data handling and good information governance

All staff will be trained on data handling, security and appropriate information governance. All training will be coordinated by the Data Protection Officer and the Information Compliance Manager, who will ensure there is an auditable record of training completion.

5.8 There must be good awareness of data protection and data security

The Data Protection Officer will ensure that there is an ongoing mechanism for maintaining good awareness of information governance matters. This will comprise:

a) Updated information on the council's intranet (izzi)
b) Promoting the Data Protection training course
c) Attending Departmental Management Team meetings
d) Training specific groups of staff within specialist areas
e) Classroom training for those staff without routine access to the council's network

6 POLICY COMPLIANCE

All staff are expected to serve the council and implement its policies to the highest standards, as described in the Code of Conduct. If any user is found to have breached this policy, they may be subject to the council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s). If you do not understand the implications of this policy or how it may apply to you, please seek advice from the Information Governance Team.

7 GOVERNANCE, APPROVAL AND REVIEW

7.1 Corporate Governance Group

This policy and the commitment to a robust governance framework is subject to continuous, systematic review and improvement. This council-wide policy will be governed by the Corporate Governance Group (CGG), chaired by the Director of Resources, who is also the council's Senior Information Risk Owner. The CGG has clear terms of reference and reports directly into the Corporate Management Board.

7.2 Formal approval, adoption and review

This policy will be formally signed off by the Corporate Management Board. It will be reviewed on an annual basis by the Data Protection Officer who will feed back any issues to CGG.

7.3 The signatories agree with the content of this document.

Name	Role	Signature	Date Signed
Mike Curtis	Senior Information Risk Owner and Chair of the Corporate Governance Group		
Shona Nicolson	Head of Information Governance and Business Support		
Leila Ridley	Information Compliance Manager		
	Data Protection Officer		