Islington Data Protection Policy
A council-wide information policy
Version 1.1
June 2014
Copyright Notification

Copyright © London Borough of Islington 2014

This document is distributed under the Creative Commons Attribution 2.5 license. This means you are free to copy, use and modify all or part of its contents for any purpose as long as you give clear credit for the original creators of the content so used. For more information please see: http://creativecommons.org/licenses/by/2.5/

Contacts

If you need any further information about this document or any clarity about the contents of the document, please contact: Sinead Mulready (Data Security Manager).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Reason for change</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>13 May 2012</td>
<td>0.1</td>
<td>First draft</td>
<td>Sinead Mulready</td>
</tr>
<tr>
<td>6 June 2012</td>
<td>0.2</td>
<td>Reviewed by Peter Fehler</td>
<td>Sinead Mulready</td>
</tr>
<tr>
<td>6 June 2012</td>
<td>0.3</td>
<td>Reviewed by Jeremy Tuck</td>
<td>Sinead Mulready</td>
</tr>
<tr>
<td>12 June 2012</td>
<td>0.4</td>
<td>Reviewed by Robin Ingram (Hytec)</td>
<td>Sinead Mulready</td>
</tr>
<tr>
<td>20 June 2012</td>
<td>0.5</td>
<td>Reviewed by Jeremy Tuck</td>
<td>Sinead Mulready</td>
</tr>
<tr>
<td>02 August 2012</td>
<td>0.6</td>
<td>Changes incorporated following CAB and DSWG consultation review</td>
<td>Jeremy Tuck</td>
</tr>
<tr>
<td>September 2012</td>
<td>1.0</td>
<td>Approved by Audit Committee and published on website</td>
<td>Sinead Mulready</td>
</tr>
<tr>
<td>June 2014</td>
<td>1.1</td>
<td>Annual review</td>
<td>Sinead Mulready</td>
</tr>
</tbody>
</table>

Distribution:

This document has been distributed to:

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peter Fehler</td>
<td>Service Director Corporate and Dispute Resolution</td>
</tr>
<tr>
<td>Mike Smith</td>
<td>Chief Corporate &amp; Litigation Lawyer</td>
</tr>
<tr>
<td>Jeremy Tuck</td>
<td>Head of ICT Transformation and Assurance</td>
</tr>
<tr>
<td>CAB Board and DSWG</td>
<td>Boards and groups responsible for corporate data security and setting data protection policy</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

1 PURPOSE OF THIS DOCUMENT ..................................................................................................4
2 WHAT IS PERSONAL DATA? .......................................................................................................4
3 BACKGROUND ..............................................................................................................................4
4 APPLYING THE POLICY ...............................................................................................................4
   4.1 THE COUNCIL MUST BE A REGISTERED DATA CONTROLLER ........................................4
   4.2 THE COUNCIL MUST PROCESS PERSONAL DATA IN ACCORDANCE WITH THE ACT ....5
   4.3 THE COUNCIL WILL HAVE A FAIR PROCESSING NOTICE ................................................5
   4.4 DATA SUBJECTS CAN ACCESS INFORMATION HELD ABOUT THEMSELVES ..............6
   4.5 THE COUNCIL MUST ENSURE THAT PERSONAL DATA ARE ACCURATE .....................6
   4.6 THE COUNCIL MUST STORE DATA SECURELY ..............................................................6
   4.7 THE COUNCIL MUST ENSURE THAT STAFF UNDERSTAND THEIR RESPONSIBILITIES ..6
   4.8 INFORMATION SHARING AGREEMENTS .....................................................................7
5 ROLES AND RESPONSIBILITIES .................................................................................................8
   5.1 OVERVIEW .........................................................................................................................8
   5.2 CORPORATE MANAGEMENT BOARD WILL RECEIVE REPORTS ON DATA PROTECTION AND SECURITY 8
   5.3 THE CORPORATION GOVERNANCE GROUP WILL RECEIVE REPORTS ON DATA PROTECTION AND SECURITY ................8
   5.4 THE ICT TRANSFORMATION AND ASSURANCE TEAM WILL RAISE RISKS AS APPROPRIATE ....8
   5.5 SERVICE AREAS MUST BE REPRESENTED AT INFORMATION GOVERNANCE OFFICER MEETINGS ....9
   5.6 SERVICE AREAS MUST BE REPRESENTED AT THE DATA SECURITY WORKING GROUP ..........9
   5.7 ALL STAFF MUST BE TRAINED ON DATA HANDLING AND GOOD INFORMATION GOVERNANCE ..........9
   5.8 THERE MUST BE GOOD AWARENESS OF DATA PROTECTION AND DATA SECURITY ............9
6 POLICY COMPLIANCE ..................................................................................................................9
7 GOVERNANCE, APPROVAL AND REVIEW ..............................................................................10
   7.1 CORPORATE GOVERNANCE GROUP .............................................................................10
   7.2 FORMAL APPROVAL, ADOPTION AND REVIEW .............................................................10
   7.3 THE SIGNATORIES AGREE WITH THE CONTENT OF THIS DOCUMENT..........................11
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 1998 is: data which relates to a living individual who can be identified from that information or from those data and other information in the possession of, or likely to come into the possession of, the council. This may include, but is not limited to, the name of a living person and data associated with that name.

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 1998.

The council is committed, as a general rule, to processing personal data according to 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 is available from the Information Commissioner's Office, at Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Telephone: 0303 123 1113 or 01625 545745. Web: www.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. The Data Protection Act defines a data controller as a (legal) person who determines the purposes for which and the manner in which personal data are processed or are to be processed. 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.

Heads of Service Areas are responsible for informing the Data Security Manager 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 must process personal data in accordance with the Act

The council will comply with the eight Data Protection Principles as set out in the Data Protection Act (1998) in relation to personal data that the council processes:

- Process personal data fairly and lawfully and with justification under one of the conditions in Schedule 2 (and, if the data are sensitive personal data, one of the conditions under Schedule 3).
- Obtain personal data only for one or more specified and lawful purposes, and not further process personal data in any manner incompatible with that purpose or those purposes.
- Ensure that personal data are adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Make sure that personal data are accurate, and where necessary, kept up to date.
- Ensure that personal data processed for any purpose or purposes are not kept for longer than is necessary for that purpose or those purposes.
- Process personal data in accordance with the rights of data subjects under the Data Protection Act. In particular, the council will supply information in response to an individual’s request under the right of access to personal information, and will comply with notices given under the right to prevent processing likely to cause damage or distress, the right to prevent processing for the purposes of direct marketing and rights in relation to automated decision-making.
- Take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Not transfer personal data to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

4.3 The council will have a Fair Processing Notice

The council will ensure that data is obtained fairly. This applies to data that is obtained in person, or by completing a paper or electronic form. The information provided will state that the council is the data controller, the purpose or purposes for which the data are intended to be processed, and any further information necessary to enable the processing to be fair, e.g. the likely consequences of the data processing and whether particular disclosures can reasonably be envisaged.

The Fair Processing Notice (FPN) is a statement by Islington Council notifying any customers who provide us with personal data, (for example, address, telephone number etc.) that such information may be processed for the purpose of completing, verifying, correcting or updating all records and computerised systems for the council. This will allow us to ‘pool’ the data of any customer who provides us with information. The statement appears on all council forms, council tax bills and any printed stationery that requests customer information. This has been standard practice since the end of 2007. Personal data must not be processed other than for the original purpose for which it was provided unless it is covered by an FPN or by another provision of the Data Protection Act.
The council’s Fair Processing Notice is available on the council website. The Fair Processing Notice states:

“Any personal information you give us is held securely and will be used only for council purposes. Information that was collected for one purpose may be used for another council purpose, unless there are legal restrictions preventing this. Islington may share this information where necessary with other organisations, including (but not limited to) where it is appropriate to protect public funds and/or prevent fraud in line with the National Fraud Initiative guidelines.

Using your information in this way allows us to deliver more efficient services that can be tailored to your individual needs and preferences. All personal information is held in strict confidence. The use of data by the Audit Commission in a data matching exercise is carried out with statutory authority under its powers in Part 2A of the Audit Commission Act 1998.”

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

4.4 Data subjects can access information held about themselves

A data subject is an individual whose personal data are controlled by a data controller. Individuals have the right of access to their personal data held by the council (subject to exemptions). The council has an Access to Information policy which provides further information about this procedure and this can found on the council’s website.

4.5 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.

4.6 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.

4.7 The council must ensure that staff understand their responsibilities

The council will ensure that:

- It has a Data Protection Manager with specific responsibility for ensuring compliance with the Data Protection Act;
- 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.

4.8 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. We use a contract when are commissioning a third party to carry out a service (or process data) on our behalf. We use an Information Sharing Agreement 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.

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 Exemptions 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.

3.2 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 (i.e., 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 RESPONSIBILITIES

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 1998.

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 Data Security Manager, who has the remit for corporate information compliance.

5.4 The ICT Transformation and Assurance 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 ICT Transformation and Assurance will determine when risks should be escalated to the Customer Access Board and will prepare reports for this board when necessary.

b) The Data Security Manager 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 Security Manager will highlight risks to the Senior Information Risk Owner.

c) The Information Compliance Manager will respond to access to information requests and
process 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 also produce reports on the council’s compliance with access to information requests and these will be submitted regularly to the Corporate Management Board.

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 Security Manager, 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 Security Manager and 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 Security Manager 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 (izzy)
- b) Promoting the Data Security 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 Digital Services.
7 GOVERNANCE, APPROVAL AND REVIEW

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

7.2 Formal approval, adoption and review
This policy has been formally approved by the council’s Audit Committee. The Data Security Manager will lead an annual review of this policy.
7.3 The signatories agree with the content of this document.

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
<th>Signature</th>
<th>Date signed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Louise Round</td>
<td>Director – Corporate Resources</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peter Fehler</td>
<td>Service Director Corporate and Dispute Resolution</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emma Marinos</td>
<td>Director of Communications and Technology</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adrian Gorst</td>
<td>Head of ICT Operational Delivery</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jeremy Tuck</td>
<td>Head of ICT Transformation and Assurance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sinead Mulready</td>
<td>Data Security Manager</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>