ISLINGTON

Information Governance Policy

A council-wide information management policy

Version 1.4
May 2019

Revision History

Date	Version	Reason for change	Author
16.5.2012	0.1	First version.	Jeremy Tuck
23.5.2012	0.2	Revisions. These include the reference in the Roles and responsibilities for a named Senior Information Risk Owner.	Jeremy Tuck
6.6.2012	0.3	Revisions.	Jeremy Tuck
6.6.2012	0.4	Revisions following comment from Sinead Mulready.	Jeremy Tuck
20.6.2012	0.5	Minor corrections and typos following review from Hytec	Jeremy Tuck
11.8.2012	0.6	Incorporated comments from CAB	Jeremy Tuck
26.4.2013	0.7	Update to version following change of personnel in the council	Leila Ridley
15.5.13	0.8	Following consultation with Director of Digital Services and Transformation	Leila Ridley
13.6.13	1.0	Following CMB approval	Leila Ridley
June 2014	1.1	Annual review	Leila Ridley
7.9.15	1.2	Annual review	Leila Ridley
01/03/18	1.3	Updated to reflect organisational and legislative changes	Leila Ridley
08/05/19	1.4	Annual review	Leila Ridley

TABLE OF CONTENTS

1 PURPOSE OF THIS DOCUMENT

This document sets out the framework within which the council will promote a culture of good practice around the processing of information and the use of information systems and details the agreed policy for achieving this.

2 SCOPE

a) Systems: All Information Systems within the organisation (both electronic and paper based) fall within the scope of this framework.

b) Staff: All users of council information and/or systems including council employees and non-council employees who have been authorised to access and use such information and/or systems.

c) Information: All information and data collected or accessed in relation to any council activity whether by council employees or individuals and organisations under a contractual relationship with the council. All information stored on facilities owned or managed by the council or on behalf of the council. All such information belongs to the council unless proven otherwise.

3 THE OVERALL GOVERNANCE FRAMEWORK

3.1 Overview

An information governance framework describes the measures in place to manage information appropriately to support the council's capacity to deliver efficient services and achieve the council's vision for a fairer Islington. The framework comprises the following:

a) Measures are in place to ensure national legal compliance

b) Stated information governance policy measures in place

c) Good information governance assurance mechanisms are in place

d) Duties and responsibilities are in place

3.2 Measures in place to ensure national legal compliance

This document sets out the council's policy towards information governance, including the council's information standards and the procedures in place to ensure the council meets legal obligations in respect of the Freedom of Information Act 2000, the Environmental Information Regulations 2004, the Re-use of Public Information Regulations 2015, Data Protection Act 2018, the General Data Protection Regulation and the statutory rules concerning access to information about council meetings and papers, including those of the Executive. This policy also sets out the governance framework, including setting out the key roles and responsibilities and the arrangements for training, monitoring and review in relation to each of these areas.

3.3 Stated information governance policy measures in place

The council will ensure that it has policy measures in place to enable good practice around the handling of information; promoting a culture of awareness and improvement; and, complying with legislation and other mandatory standards. These are described in the section 'Information Governance Policy'.

To support the council's commitment to good information governance, the council will, in addition to this policy maintain and abide by the following other information policies and procedures and these will be updated regularly.

This policy should be read in conjunction with the Digital Services Policies, which sets out the overarching approach to Information and Communication Technology (ICT) policies in Islington Council. The council also has a number of Information Governance Policies that set out the council's approach to complying with relevant legislations.

ICT Security Policies
a) ICT Security Policy Framework
b) Security Incident Policy
c) Acceptable Use Policy
d) User Management Policy
e) Physical Security of Information Policy
f) Remote Working Security Policy
g) Third Party Access Policy
h) Access Control Policy
i) Operational Network Policy

Information Governance Policies
a) Data Protection Policy
b) Access to Information Policy
c) Records Management Policy
d) Retention Schedule
e) Managing Individual's Rights Procedure
f) Information Asset Owner Policy
g) Information Risk Assessment Procedure

3.4 Good information governance assurance mechanisms are in place

The council will ensure that it has measures for monitoring information governance and escalating issues and concerns as they arise. These are described in this policy in the section 'Corporate Measures for Information Assurance'.

3.5 Clear duties and responsibilities are in place

The council will detail the roles and responsibilities that need to be in place to ensure adherence to good information governance arrangements. These are described in this policy framework under 'Roles and Responsibilities'.

4 KEY ROLES AND RESPONSIBILITIES

4.1 Corporate Governance Group

The Corporate Governance Group (CGG) is formally constituted as a reference committee to the council's Corporate Management Board (CMB) to oversee Information Governance, Security Policy Framework, information compliance and records management. CGG is chaired by the council's Senior Information Risk Owner.

4.2 The Monitoring Officer

The Director of Law and Governance

a) As monitoring officer for determining whether exemption 36 (exemption from disclosure of information which might prevent the free and frank provision of advice or exchange of views, or which would otherwise prejudice the effective conduct of public affairs) can be relied upon.

b) As statutory proper officer in relation to the access to information rules, for determining whether reports or parts of reports intended to be considered at a formal member level meeting should be marked "Not for Publication" on the basis that it is likely that the public will be excluded from the meeting when the report is considered because it contains exempt information. They are also responsible for ensuring that notices and papers are publicised as required under the rules.

c) For advising on any disputes as to a members' entitlement to information.

The Director of Law and Governance also acts as the council's Deputy SIRO.

4.3 The Senior Information Risk Owner (SIRO)

The Corporate Director of Resources serves corporately as the council's named Senior Information Risk Owner (SIRO) in relation to information governance and security related matters. The Corporate Director for Resources sits on the Corporate Management Board and reports to the Chief Executive.

The SIRO has responsibility for understanding how the strategic business goals of the Council may be impacted by information risks, and for taking steps to mitigate them. The SIRO does not act in isolation, but is supported and receives assurance from the Information Asset Owners (IAO) who assumes responsibility for their information assets and any associated risk.

The SIRO is accountable for ensuring:

- That they foster and lead an appropriate (security) culture
- The Council manages information risk
- The Council has a process for managing security incidents
- The Council has an Information risk policy
- The Council carries out an annual assurance process which includes a review of information risk
- The Council completes Data Protection Impact Assessments for new projects
- Appropriate escalation and notification to the Chief Executive, CMB and SLT on cross-cutting information risk
- The Council has a clearly documented information risk management identification and review process

SIRO is responsible for:

- Providing guidance to information asset owners
- Ensuring that IAOs have been identified for all assets and that they understand their responsibilities
- Oversight of and prioritisation of Information Governance activities
- Ensuring the information risk appetite is recorded and incorporated in the risk management process and communicated to the Council
- Making the final decision for accepting risks outside the level of acceptance, in consultation with CMB
- Sign off data flows via Corporate Governance Group
- Own information risk policies and processes

- Sign off on audit findings
- Sign off information governance and security polices
- Sign off process review findings from the Head of Information Governance and DPO

4.4 Data Protection Officer

The Head of Information Governance & Data Protection Officer serves as the council's 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.).

4.5 Information Asset Owners

All Service Directors act as Information Asset Owners (IAO) for their Service Area in relation to information assets and information risks. IAOs are responsible for ensuring that specific information assets are accessed, handled and managed appropriately. They ensure that information assets are properly protected, that risks are appropriately identified and managed and that their value to the organisation is fully exploited. Full details of their roles and responsibilities can be found in the Information Asset Owner Policy.

4.6 Information Leads

Information Leads are nominated by the IAO and provide support to the IAO to ensure the role is carried out effectively. Full details of their roles and responsibilities can be found in the Information Asset Owner Policy.

4.7 The Technical Design Authority

The Technical Design Board is a specialist group to quality assure that all system development is consistent with the ICT Strategy. The Technical Design Board acts to improve control over the way systems are tested, procured and implemented.

4.8 Information Governance Working Group

The Information Governance Working Group serves to ensure that the data and information assets of Islington Council are kept secure. Meetings are held at least four times a year and any issues are escalated to the Corporate Governance Group.

4.9 Information Governance Officers

All Directorates have nominated Information Governance Officers (IGOs) who serve to represent all aspects of access to information within their functional area, including Freedom of Information, Environmental Information Regulations and Data Protection. Meetings are held at least quarterly.

4.10 Information Governance Team

The council's Information Governance Team are responsible for ensuring the council remains compliant with the legislations referred to in this Policy, managing security incidents and ensuring that training and awareness programmes are in place so that staff are aware of and understand their obligations. The Information Governance Team are also responsible for overseeing the council's corporate records management approach in order to support the council's statutory duty under Section 224 of the Local Government Act 1972 to make "proper arrangements" for the records it creates. This team has specific responsibilities linked to roles for:

a) Information compliance management
b) Data privacy compliance
c) Data security management
d) Records management

4.11 All service areas

Each service area must ensure that it appropriately captures and stores records (both paper and electronic) that serve as evidence of its functional (business) activities. Service areas should identify appropriate Information Governance Officers in their area and must ensure compliance with the Freedom of Information Act, Environmental Information Regulations and Data Protection legislation. Service areas should observe and support the corporate standards endorsed by the Information Governance Team.

4.12 All staff

All staff are responsible for responding to information requests relating to their work as part of their day-to-day function. As part of this, all staff must be aware of how to deal with information requests under the Freedom of Information Act and the Environmental Information Regulations and requests relating to Individual's Rights as defined by the General Data Protection Regulation.

4.13 Chief Digital Information Officer

The Chief Digital and Information Officer is responsible for the delivery of the corporate Technology function, including Policy and Strategy, Operational Capacity and Performance.

5 INFORMATION GOVERNANCE POLICY

5.1 The council will comply with legislation and other mandatory standards

5.1.1 Overview

The council is committed to continuously improving the way it responds to requests for information under statutory access regimes, including the Freedom of Information Act 2000, the Data Protection Act 2018, the General Data Protection Regulation, and the Environmental Information Regulations 2004. Compliance, however, is reliant upon proper management of the council's information, which needs to be managed, secure and easily located. The council regards all identifiable personal information relating to residents as confidential and all identifiable information relating to staff as confidential (except where national policy on accountability and openness requires otherwise). The council complies with the Data Protection Act 2018, General Data Protection Regulation, the Freedom of Information Act and the common law of confidentiality.

5.1.2 Freedom of Information

The Freedom of Information Act 2000 (FOIA) together with the Environmental Information Regulations 2004 (EIR) provide the public a general right of access to information held by the council. When a written request for information is made, the council must provide a response within 20 working days. If the council holds a record of the information on any record system (even backup systems and off-site storage archives) then the council must either provide the requestor with the information, or must state which exemption has been applied. Delivering this right of access efficiently to the public can only be achieved with efficient, well managed records management systems.

5.1.3 Environmental Information Regulations

Islington Council is legally bound to deal with requests for information that are covered by the EIR. Environmental information covers information on the state of the environment, such as air, water, soil, land, flora and fauna and diversity and will also include information on genetically modified organisms. In addition, information on emissions and discharges, noise, energy, radiation, waste and other such substances; measures and activities such as policies, plans and agreements; reports, cost benefit and economic analyses are included. The state of human health and safety, contamination of the food chain; cultural sites and built structures as they may be affected by environmental factors, will also be considered environmental information. The EIR are aligned with FOIA in many ways. Therefore, at Islington, both sets of regulations are dealt with under the same process. The key to this process is that: a response to all requests for information must be provided within 20 working days. Information can only be withheld when allowed (or required) to do so by specific exceptions granted to us by law.

5.1.4 Data Protection Act 2018 and the General Data Protection Regulation

The Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR) requires all organisations that handle personal information to comply with six data protection principles including in relation to privacy and disclosure. These principles relate to the: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation and; integrity and confidentiality.

The council will maintain a Data Protection Policy and an Individual's Rights Handling Policy and procedures. These documents will set out what the individual's rights are and explains the process for enacting or utilising these rights. The process for accessing Individual's Rights and forms for requesting information is available on the public website.

5.1.5 Local Government (Records) Act 1962

The Local Government (Records) Act 1962 gave local authorities limited discretionary powers to hold their records in local archives. In particular, the Act states that: 'A local authority may do all such things as appear to it necessary or expedient for enabling adequate use to be made of records under its control'.

5.1.6 Local Government Act 1972

The Local Government Act 1972 set out the basic requirement for local authorities to 'make proper arrangements' to keep good records.

5.1.7 Lord Chancellor's Code of Practice for Records Management

The Lord Chancellor published a Code of Practice for records management in 2002 (revised in 2009) as a supplement to the Freedom of Information Act (mentioned above) that all public bodies should follow. Section 7 states that 'Authorities should have in place a records management policy, either as a separate policy or part of a wider information or knowledge management policy.'

5.2 The council will promote open information

5.2.1 Overview

The council will promote open information and has described these objectives in the Data Strategy. The council will consider developing a culture where there is an open and transparent, public approach to release data the council officers create unless there are clear legal restrictions not to do so. The council will develop its data strategy which will include how data will be published and protectively marked according to risk and sensitivity.

5.2.2 Access to Information Policy

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 information requests, as well as to ensure there is greater openness of decision-making; that the council builds the trust of the public; and to provide clarity on the way in which the council will meet its duties under access to information legislation, guidance and best practice.

5.2.3 Individual's Rights Handling Policy and Procedure

The council will maintain an Individual's Rights Handling Policy 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 2018 and the General Data Protection Regulation, guidance and best practice.

5.2.4 Publication scheme

The Publication Scheme provides a listing of documents routinely requested by the public. It is organised into 'classes' of information that are easy to understand. The Publication Scheme is produced directly from documents held on the website and can be located in the council's records library.

5.2.5 Re-use of information policy

The Re-use of Public Sector Information Regulations 2015 implement the European Directive (2013/37/EU) on the re-use of information. The focus of the Regulations is on re-use rather than access – and the regulations do not provide access to the information itself. The Regulations require the council to ensure that a list of significant documents available for re-use is made available to the public, preferably by electronic means and, as far as reasonably practicably, with an electronic search capability. However, the Regulations do not provide access to the information itself. Requests for access to information will still be dealt with under the FOIA, DPA, GDPR, EIR and numerous other information access provisions.

5.2.6 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, individual's will be able to access service specific privacy notices.

5.3 The council will commit to information security and confidentiality

5.3.1 Physical and electronic assets

The council is committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout Islington Council. Information and information security requirements will continue to be aligned with council's goals and the framework of security policies is intended to be an enabling mechanism for information sharing, electronic operations, and reducing information-related risks to acceptable levels. In particular, business continuity and contingency plans, data back-up procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to the success of this policy.

The diffusion of technology into our daily working environment has meant that data security has become a Corporate Management Board issue. There is more focus on the transparency of public data than ever before with the intention that publishing data will strengthen accountability to citizens. At the same time, central government data losses and the continuing emphasis in the press around breaches of data security required the council to reinvigorate its response to data security.

5.3.2 Security Policy Framework

This policy should be read in conjunction with the 'Shared Digital ICT Security Policy Framework', which sets out the overarching approach to Information and Communication Technology (ICT) policies in Islington Council. These are listed in the Overall Framework section of this policy.

6 MEASURES IN PLACE FOR INFORMATION ASSURANCE

6.1 Overview

Information assurance describes the measures that are in place to ensure that the council meets the requirements for good information governance. This section, therefore, describes how the roles and governance arrangements will operate to ensure that this is achieved.

6.2 Corporate Management Board will receive reports on information governance

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. The Corporate Management Board will also receive routine reports on the council's progress on Access to Information requests. These will be submitted by the Head of Information Governance & Data Protection Officer.

6.3 The Corporate Governance Group will receive reports on information governance

The Corporate Governance Group will operate with a forward plan and will receive reports on improved data assurance, records management processes and monitor risks relating to information governance

issues. Reports will be submitted by the Information Governance Team, who has the remit for corporate records management and information compliance.

6.4 The Information Governance team will raise risks as appropriate

The Information Governance Team will raise risks related to information governance and report these as appropriate:

a) The Information Governance Team will determine when risks ought to be escalated to the Corporate Governance Group and will prepare reports for this board when necessary.

b) The Head of Information Governance & Data Protection Officer will respond (reactively) to data security incidents as they arise and manage a process of improvement (proactively) through the Information Governance Working Group. The Head of Information Governance & Data Protection Officer will also provide assurance by advising the Technical Design Authority and highlight risks to the SIRO.

c) The Access to Information Manager has corporate responsibility for access to information requests and information complaints and will determine the processing of these in accordance with the council's responsibilities for records management. The Access to Information 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 SIRO. The Access to Information 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.

6.5 Service areas will be represented at Information Governance Officer meetings

Service areas will ensure that there is appropriate representation at the council's Information Governance Officer meetings and will raise issues related to information management, and access to information where appropriate. Any issues raised at these meetings will be escalated by the chair of the meeting, the Access to Information, who will raise these matters with the Head of Information Governance & Data Protection Officer and SIRO where necessary.

6.6 Service areas will be represented at the Information Governance Working Group

Service areas will ensure that there is appropriate representation at the council's Information Governance Working Group and will support the council by ensuring their areas remain compliant with data protection legislation. Members will raise issues related to compliance with legislation, including data and records management; data security; data breaches; and training requirements where appropriate. Any issues raised at these meetings will be escalated by the chair of the meeting, the Head of Information Governance & Data Protection Officer, who will raise these matters with the SIRO where necessary.

6.7 Routine Technical Design Authority meetings will be held

Fortnightly Technical Design Authority meetings are held to review any new systems that are being introduced into the council. A clear process exist for submitting reports, maintaining an issues log and recording technical decisions. All issues raised at this meeting will be escalated by the chair of the meeting, the Solutions Architect, who will produce a Statement of Risk and escalate this appropriately.

6.8 All staff will 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 Information Governance Team, who will ensure there is an auditable record of training completion.

6.9 There will be good awareness of information governance matters

The Information Governance Team 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 Security training course

c) Attending Departmental Management Team meetings

d) Training specific groups of staff within specialist areas

6.10 A records management policy will be maintained

The council will maintain a records management policy which sets out a corporate policy for the management of records within Islington Council to ensure compliance with the Local Government Act 1972, Data Protection Act 2018, the General Data Protection Regulation and the Freedom of Information Act 2000. The policy defines roles and responsibilities and sets out the standards of corporate records management (retention schedule, classification scheme, corporate EDRM and records destruction). The Records Management Policy will be reviewed annually by the Information Governance Team and approved by the Corporate Governance Group.

6.11 A Corporate Records Retention Schedule will be maintained

The retention schedule sets how long records need to be stored before we can or should destroy them. The council's retention schedule is built on the retention periods given in the Local Government Classification Scheme (LGCS). Changes to these retention periods, where required, will be approved between service areas and the Information Governance Team and Legal Services. The retention schedule will be reviewed annually by the Information Governance Team and approved by the Corporate Governance Group.

6.12 A Corporate Classification Scheme will be maintained

Records should be stored where possible using a functional (rather than organisational) filing system, based around what services the council provide rather than by the name of the team. Details of the council's records, paper or electronic, will be recorded in the Islington classification scheme. The scheme divides records into 'classes', with appropriate retention periods and access controls recorded for each class. The Corporate Classification Scheme will be updated routinely by the Information Governance Team and approved by the Corporate Governance Group.

6.13 The council will maintain the DSP Toolkit

The DSP Toolkit is a performance tool produced by NHS Digital. It draws together the legal rules and central guidance of Information Governance and presents them in one place as a set of Information Governance requirements. Organisations are required to carry out self-assessments of their compliance against the DSP requirements including: requirements for management structures and responsibilities (e.g. assigning responsibility for carrying out the Information Governance assessment, providing staff training etc.); confidentiality and data protection; and Information security.

The Information Governance Team will complete and submit the council's DSP Toolkit submission annually. Any department requiring access to the council's Connection to Health systems will provide the resources to work with the Information Governance Team to develop appropriate procedures, training and evidence for their department. They must ensure that their department's evidence is fit for purpose, and reviewed and updated annually.

7 REPORTING INCIDENTS

All faults, security incidents or breaches of data must be reported Digital Services via ICT HelpMe in line with council policy. It is the duty of all council staff and all other users of council equipment to immediately report any actual or suspected breaches in information security to the Information Governance Team.

8 POLICY COMPLIANCE

All employees 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.

9 GOVERNANCE, APPROVAL AND REVIEW

9.1 Corporate Governance Group

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

9.2 Formal approval, adoption and review

This policy will be formally signed off by Corporate Management Board. It will be reviewed on an annual basis by the Information Governance Team and approved by the Corporate Governance Group.

Name	Role	Signature	Date Signed
Nicki Beardmore	**Interim Corporate Director of Resources**		
Peter Fehler	**Acting Director of Law and Governance**		
Leila Ridley	**Head of Information Governance and Data Protection Officer**		
Antoinette Carter	**Data Protection Lead**		
Brad Pearton	**Access to Information Officer**		
Jon Cumming	**Interim Chief Digital Information Officer**		
VACANT	**Head of Cyber Security**		

10 APPENDIX A