Information Governance Policy Framework

Version 2, February 2024

Revision history

Date	Version	Summary of action	Author
May – Aug 2012	0.1 – 0.6	Policy creation	Jeremy Tuck
June 2013	1.0	Annual review	Leila Ridley
June 2014	1.1	Annual review	Leila Ridley
September 2015	1.2	Annual review	Leila Ridley
March 2018	1.3	Updated to reflect organisational and legislative changes	Leila Ridley
May 2019	1.4	Annual review	Leila Ridley
December 2020	1.5	Annual review	Leila Ridley
December 2021	1.6	Annual review	Leila Ridley
December 2023	1.7	Creation of IG Framework document	Leila Ridley
February 2024	2.0	New framework adopted and published	Leila Ridley

Table of Contents

1. Purpose and scope

This document sets out the Information Governance Framework for Islington Council. The framework is applicable to Islington Council employees, agency staff, councillors, volunteers, contractors, service providers and other organisations or agencies working for or on behalf of the council.

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

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.

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.

2. The overall governance framework

2.1 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.

2.2 Measures in place to ensure 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 UK General Data Protection Regulation (UK GDPR) 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.

2.3 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 has several Information Governance Policies that set out the council's approach to complying with relevant legislations.

Information Governance Policies

- Data Protection Policy
- Data Breach Policy
- Appropriate Policy Document
- Data Handling Policy
- Access to Information Policy
- Records Management Policy
- Retention Schedule
- Information Asset Owner Procedure
- Information Risk Assessment Procedure

This policy should be read in conjunction with the Islington Digital Services Policies, which sets out the overarching approach to Information and Communication Technology (ICT) policies in Islington Council.

2.4 Information 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'.

2.5 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'.

3. Accountability Principle

3.1 Information Governance Board

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

The IG Board receive updates on the progress against agreed actions to support the delivery of the Information Governance Strategy and any data protection audits that have taken place.

3.2 The Monitoring Officer

The Director of Law and Governance serves as the council's monitoring officer and will have responsibility for:

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.

3.3 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 ensures that the council fosters and leads an appropriate security culture and is accounting for ensuring that the council:

- Manages information risk and ensures that this is reviewed at least annually.
- Has a process for managing security incidents and data breaches.
- Has an Information risk policy and clearly documented information risk management identification and review process in place.
- That Data Protection Impact Assessments are completed on high-risk projects.
- That Chief Executive and CMT are notified on information risk where appropriate.

The SIRO is responsible for ensuring:

- That IAOs have been identified for all assets and that they understand their responsibilities.
- That there is oversight of and prioritisation of Information Governance activities at a corporate level.
- That information risk decisions are made and has the final decision for accepting risks outside the level of acceptance, in consultation with CMT.
- That the organisation is compliant with its transparency obligations under the Access to Information legislations.

3.4 Data Protection Officer

The Assistant Director of Information and Digital Governance 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 can report directly into CMT 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.).

3.5 Caldicott Guardian

The Director of Adult Social Care will serve as the council's Caldicott Guardian. The Caldicott Guardian helps the council to ensure that confidential information about health and social care serve users is used ethically, legally and appropriately ensuring service user's right to confidentiality.

3.6 Director of Digital Services

The Director of Digital Services is responsible for the delivery of the corporate technology function, including setting the strategic approach and ensuring that there is operational capacity and performance. The Director of Digital Services shall ensure that there is high awareness of cybersecurity threats.

3.7 Information Asset Owners

All members of CMT are responsible for ensuring that Information Asset Owners (IAO) have been identified for their directorates. IAOs are responsible for ensuring, Information Leads are identified and that information assets are accessed, handled and managed appropriately. Full details of their roles and responsibilities can be found in the Information Asset Owner procedure.

IAOs must attend training in information asset management and refresh their understanding every two years.

IAOs are responsible for arranging quarterly meetings with the Information Governance (IG) team. Any issues raised at these meetings will be escalated by the chair of the meeting, the Assistant Director of Information and Digital Governance, who will raise these matters with the SIRO where necessary.

3.8 Information Leads

Information Leads are nominated by the IAO and provide support to the IAO to ensure the role is carried out effectively whilst ensuring that information risk is raised effectively.

Information Leads must attend training in information asset management and refresh their understanding every two years and attend quarterly meetings.

Full details of their roles and responsibilities can be found in the Information Asset Owner procedure.

3.9 The Technical Design Board

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.

3.10 Information Asset Owner Meetings

IAO meetings will be held quarterly with the IDG team to ensure that the data and information assets of the council are kept secure. Meetings focus on key areas of work or risks to compliance; significant issues are escalated to the IG Board.

3.11 Information and Digital Governance Team

The council's IDG Team are responsible for ensuring the council remains compliant with the legislations referred to in this framework, managing data breach investigations and ensuring that training and awareness programmes are in place so that staff are aware of and understand their obligations. The IDG Team are also responsible for overseeing the council's corporate records management approach 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:

- Information compliance management
- Managing the council's transparency obligations under the Access to Information legislations including responsibility for responding to all requests made under the Access to Information legislations and UK GDPR
- Information complaints management
- Data privacy compliance
- Data breach investigations
- Records management
- Information Governance training and awareness

3.12 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 must ensure compliance with the Freedom of Information Act 2000 (FOIA), Environmental Information Regulations 2004 (EIR) and Data Protection legislations. Service areas should observe and support the corporate standards endorsed by the IDG Team.

3.13 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 FOIA and EIR and requests relating to Individual's Rights as defined by the UK GDPR.

4. Information governance policy

4.1 The council will comply with law and other mandatory standards

4.1.1 Overview

The council is committed to continuously improving the way it responds to requests for information under statutory access regimes, including the FOIA, EIR, Data Protection Act 2018, and UK GDPR. 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, UK GDPR, FOIA, EIR, the Code of Transparency and the common law of confidentiality.

4.1.2 Freedom of Information and Environmental Information Regulations

The FOIA together with the 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.

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.

How the council manages these requests is set out in the Access to Information Policy and is available on the council's website.

4.1.3 Data Protection Act 2018 and the UK General Data Protection Regulation

The Data Protection Act 2018 (DPA) and the UK GDPR sets out seven data protection principles that the council must comply with then processing personal information. These principles ensure that personal data is only collected, used and stored when it is: lawful, fair and transparent. The council is accountable for ensuring ensure that only the data required is collected and used for the purpose limitation originally intended. Data must remain accurate and only be stored for as long as necessary. The council must ensure that data integrity is maintained and kept confidential.

The council will maintain a Data Protection Policy and an Access to Information Policy 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.

4.1.4 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'.

4.1.5 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.

4.1.6 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 FOIA 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.'

4.1.7 Local Government Code of Transparency 2015

The Local Government Code of Transparency was issued to increase democratic accountability by making it easier for local people to contribute to the local decision-making process and help shape public services. The Local Government Code of Transparency sets out both the information that must be published by local authorities and the frequency that this information must be made available.

4.1.8 Re-use of Public Sector Information Regulations 2015

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, UK GDPR, EIR and numerous other information access provisions.

4.2 The council will promote open information

4.2.1 Overview

The council will promote open information and will describe these objectives in an Open Data Strategy. The council will develop 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.

4.2.2 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, including requests for personal data, 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.

4.2.4 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.

4.2.5 Privacy Notice

The UK 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 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 will be able to access service specific privacy notices.

4.3 The council will commit to information security and confidentiality

4.3.1 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. 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.

4.3.2 Security Policy Framework

This policy should be read in conjunction with the 'Islington Digital Services ICT 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.

5. Measures in place for information assurance

5.1 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.

5.2 CMT will receive reports on information governance

The Corporate Management Team (CMT) will receive reports that relate to information governance and data and cybersecurity as appropriate. These will be presented by the chair of the Information Governance Board, who will also serve as the council's Senior Information Risk Owner (SIRO). CMT will also receive routine reports on the council's compliance with Access to Information requests.

5.3 The Information Governance Board will receive reports on information governance

The Information Governance Board will operate with strategic action 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 IDG team, who has the remit for corporate records management and information compliance.

5.4 The IDG team will raise risks as appropriate

The IDG team will raise risks related to information governance and report these as appropriate:

a) The IDG team will determine when risks ought to be escalated to the IG Board and will prepare reports for this board when necessary.

b) The Assistant Director of Information and Digital Governance will respond (reactively) to data breaches as they arise and manage a process of improvement (proactively) through the Information Asset Owner meetings. The Assistant Director of Information and Digital Governance will also provide assurance by advising the Technical Design Board and highlight risks to the SIRO.

c) The Access to Information Manager is responsible for managing the council's approach to access to information requests and ensures that these are processed according to the council's responsibilities. The Access to Information Manager will provide assurance by providing reports on the council's compliance with access to information requests and these will be submitted regularly to CMT and IG Board.

5.5 Technical Design Board meetings will be held

Weekly Technical Design Board meetings are held to review any new systems that are being introduced into the council. A clear process exists 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, Chief Technology Officer, who will produce a Statement of Risk and escalate this appropriately.

5.6 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 via mandatory eLearning. All training will be coordinated by the IDG team, who will ensure there is an auditable record of training completion.

5.7 There will be good awareness of information governance matters

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

- Updated information on the council's intranet
- Promoting the Data Protection and Information Governance training courses
- Attending Departmental Management Team meetings
- Training specific groups of staff within specialist areas

5.8 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, DPA 2018, the UK GDPR and FOIA. The policy defines roles and responsibilities in relation to the Record of Processing Activities (ROPA) and sets out the standards of corporate records management (retention schedule, classification scheme, and records destruction).

5.9 A retention schedule will be maintained

The retention schedule sets how long records need to be stored before we can 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 IDG team and, where necessary, Legal Services. The retention schedule will be reviewed annually by the IDG team and changes approved by the IG Board.

5.10 A classification scheme will be developed

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. To ensure effective management of the council's records, paper or electronic, a classification scheme will be developed. The scheme will identify the appropriate retention periods and access controls recorded for each aspect of the scheme. The classification scheme will be approved by CMT. Subsequent updates will be managed by the IDG team and approved by the IG Board.

5.10 The council will maintain the DSP Toolkit

The council will maintain the DSP Toolkit (DSPT) so that it is able to connect to Health systems. The DSPT 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. The council is required to carry out a self-assessment of

its compliance against the DSPT which includes 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 IDG team will coordinate and submit the council's DSPT submission annually. Any department requiring access to the council's Connection to Health systems will provide the resources to work with the IDG 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.

6. Reporting Incidents

All faults, security incidents must be reported via ICT Help Me. Breaches of data must be reported via iCasework 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 for investigation.

7. 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 IDG team by emailing DP@islington.gov.uk.

8. Governance, approval and review

8.1 Information Governance Board

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

8.2 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 the IG Board.

The signatories agree with the content of this document.

Name	Role
Dave Hodgkinson	Corporate Director of Resources and SIRO
Alison Stuart	Director of Law and Governance and Monitoring Officer
John Everson	Director of Adult Social Care and Caldicott Guardian
Jon Cumming	Director of Digital Services
Leila Ridley	Assistant Director of Information and Digital Governance
Mobeen Zafar	Chief Technology Officer