ISLINGTON

Records Management Policy

A council-wide policy for records management

Version 1.2

May 2019

Revision History

Date	Version	Reason for change	Author
16.6.2012	0.1	The requirement to replace the 'Records and Information Governance Strategy 2006-2009' and meet the need of the Information Governance Framework.	Jeremy Tuck
17.6.2012	0.2	Further development and input from S. Mulready	Jeremy Tuck
5.8.2012	0.3	Comments from L. Ridley	Jeremy Tuck
11.8.2012	0.4	Incorporated final comments	Jeremy Tuck
14.5.2013	0.5	Updated following changes to personnel	Leila Ridley
19.2.2014	0.6	Updated any final changes and incorporating comments	Leila Ridley
14.10.2015	0.7	Updated before final sign off by CGG	Leila Ridley
27.11.2015	1.0	Approved by CGG	Leila Ridley
01/03/18	1.1	Annual review	Leila Ridley
08/02/19	1.2	Annual review	Lisa Ford

Distribution:

This document has been distributed to:

Version	Name	Role
0.1–0.2	N3 Project team	Responsible for the delivery of the Information Governance Toolkit
0.3-0.5	DSWG and CAB	
0.6	Information Governance Team	
0.7	CGG	
1.0	All staff	Published to intranet
1.1	CGG and all staff	For approval and action
1.2	CGG and all staff	For approval and action

TABLE OF CONTENTS

1 PURPOSE OF THIS DOCUMENT

This policy document sets out the council-wide policy for records management standards that should be adhered to by all staff working with Islington Council records.

This policy should be read in conjunction with the 'Digital Services ICT Security Policy Framework', the 'Information Governance Policy', the 'Information Asset Owner Policy' and the 'Maintaining Islington's Information Asset Register Policy'.

2 INTRODUCTION

Any evidence of Council business activity is a record. Records, therefore, can be paper documents, electronic files, emails, databases, maps or images.

Records are the Council's corporate memory and provide the evidence of the Council's business actions and decisions. They also provide evidence that the Council has satisfied statutory requirements. Well managed records can improve the process of decision-making and facilitate business administration. They are, therefore, a corporate asset.

A record is a piece of information that has an intrinsic worth which makes it important enough to save and keep secure for its evidential value. In order to decide whether a piece of information is a record or not, its business context must be understood as well as its relevance and significance to the organisation (MoReq2010).

If a record is of value as evidence of business activity, it is important that it is managed in a way that ensures the record:

- Can be easily and quickly retrieved
- Is authentic – it is what it purports to be
- Is reliable – information in the record is accurate and can be depended on
- Has integrity – it is complete and unaltered
- Has appropriate context information about where it was used
- Has structure so that the record is intact

Keeping records and managing them appropriately in a way that meets the Council's legal obligations is the responsibility of all staff.

2.1.1 What is not a record?

All business activities that deliver the Council's functions are within the scope of this policy. It is important that non-records are actively managed so that they can be easily retrieved and disposed of as soon as they are no longer required.

However, what is out of scope of this policy are the following:

- Reproduced documents kept for supply purposes where master copies have been retained already;
- Books, periodicals, newspapers being kept for reference purposes;
- Duplicate copies of documents kept for convenience; and
- Personal materials which have no relation to official duties.

3 LEGISLATION

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, securely 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, the General Data Protection Regulation, the Freedom of Information Act 2000 and the common law of confidentiality.

3.1 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 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.'

3.2 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 which handle personal information to comply with six principles regarding privacy and disclosure. Particularly relevant to records management is the fifth principle, which states that 'Personal information shall be 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.'

3.3 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'.

3.4 Local Government Act 1972

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

4 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 the development and implementation of Information Governance, Data Security and Internal Audits. Specifically, CGG is responsible for:

- Ultimate approval of records, data and information policies
- Advising on serious issues around records management

4.2 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 SIRO understands the strategic business goals of the Council and how business goals may be impacted by information risks, and how those risks may be managed. The SIRO implements and leads the Information Governance risk assessment and management processes within the Council and advises CMB on the effectiveness of information risk management. Duties include:

- Taking ownership of the organisation's information risk register
- Acting as a champion for information risk at CMB
- Providing written advice on the Council's statement of internal control in regard to information risk

4.3 Information Asset Owner

Information Asset Owners (IAO) are senior members of staff, usually Service Director Level or above.

The post holder will have the skills, resources and authority to discharge the responsibilities and take action on any deficiencies in the relevant processes. The IAO has five core responsibilities, however, it is recognised that Information Leads will support delivery of these. Full details of these responsibilities can be found in the Information Asset Owner Policy.

IAOs are responsible for making arrangements to:

- Ensure the capture of records (both paper and electronic) that provide evidence of its functional activities
- Make every effort to provide reliable data and records management
- Observe and support the corporate standards endorsed by the Information Governance Team
- Understand and risk assess any service led requirement to deviate from the council's standards
- Ensure that any contractors or third parties are managing Council records effectively

4.4 Information Lead

An Information Lead should understand the overall business goals of the organisation and the importance of the information assets in supporting these goals. Information Leads should understand the IAOs five core responsibilities and lead in ensuring the methods are fully exploited to support delivery. Full details of these responsibilities can be found in the Information Asset Owner Policy.

4.5 Information Governance Working Group

The Information Governance Working Group serves to ensure that the data and information assets of Islington Council are kept secure, the Council is compliant with GDPR and Data Protection legislation and that Council records are managed effectively. Meetings will be held at least four times a year and any issues escalated to the CGG.

4.6 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.

4.7 Data Protection Officer

The Data Protection Officer 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.).

4.8 Information Management Lead

The Information Management Lead takes responsibility 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. The Information Management Lead will ensure that annual assurance is provided to the SIRO as set out in the Maintaining the Information Asset Register Policy.

4.9 Technical Design Authority

The Technical Design Authority (TDA) takes responsibility for ensuring that all Council ICT systems are designed and maintained to meet the Council's security and data protection obligations, and ensure that they are strategically and operationally fit for purpose. Changes to ICT systems are assured by Solution Architects working to the Council's ICT Enterprise Architecture Principles, patterns and design standards. These standards are also governed by TDA. The TDA refers issues of information compliance and records management to the Information Governance Team and weighs its decisions on their advice. The TDA follows the DPA and GDPR, and Information Governance best practice and IT security standards.

4.10 All staff in 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 observe and support the corporate standards endorsed by the Information Governance Team.

5 THE POLICY

5.1 Overview

This section comprises the core policy statements and commitments that the Council has made with regard to this policy.

5.2 There is a Business Classification and Retention Schedule

An important element of records management is classification. ISO 15489 defines classification as the "systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods, and procedural rules represented in a classification system". In this model classification is concerned with providing the business context for a record.

Islington Council content is based around a variant of the Local Government Classification Scheme. The Islington variation is a three tier classification comprising the elements: Function, Records Group and then Records Type.

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 retention schedule sets how long records need to be stored before we can or should destroy them. Changes to these retention periods, where required, will be approved between service areas, the Head of Information Governance and Data Protection Officer and Legal Services. Records will only be kept for as long as their contents have operational value and for as long as they may be required as evidence of the transactions they document.

5.3 There is an Information Asset Register

The Council has an Information Asset Register (IAR) that identifies the Information Assets owned by the Council. The IAR is subject to an annual review and any risks identified will be reported to the SIRO and appropriately monitored and managed by the IAO and Information Lead.

5.4 The Council will have clear Information Architecture

The Council will ensure that a clear Information Architecture is in place and this sets out the requirements for records to be stored in approved systems, media and location. This architecture will prescribe approved systems for each type of record.

5.5 There will be a corporate EDRM

There are many different systems supporting the business activities that staff do to deliver their work. These are all, by definition, records management systems, sometimes referred to as 'Line of Business Systems'. In addition, however, the Council will continue to move forward with a corporate EDRM that either complements these systems, serves to migrate unstructured data alongside these processes, or, in some cases actually does replace these systems.

5.6 Email accounts and personal drives will not be used to store council information

Staff should only store case work or other council information in the location agreed by their Information Asset Owner. This will usually be the specific system used by that department or Service Area or another corporately agreed secure location within the Council's network.

5.7 Scanning

All scanning will be undertaken according to the 'Minimum Standards for scanned documents' procedure. This document sets out minimum standards of image quality and indexing for

scanning paper records into electronic format. It is intended to ensure that the Council complies with the Code of Practice for legal admissibility and evidential weight of information stored electronically (BSI document: BIP 0008).

All paper records that service areas wish to dispose of once they have been scanned will need to meet these Minimum Standards for scanned documents in order to provide appropriate assurances that the integrity of the record has been maintained.

5.8 Storing records offsite

All records that are kept offsite will be held and managed according to the corporate classification scheme and kept according to agreed periods in the retention schedule.

5.9 The Council will adopt an archive selection policy

The Council will implement an archive selection policy that will set out how documents should be appraised for permanent archival preservation, specify the selection criteria and set out which archival institutions should be used.

5.10 The Council will ensure Digital Preservation is in place

The Council will set out the preferred use of long-term formats, formation conversion and ensure that other preservation methods are identified to prevent records becoming unusable in the future.

5.11 The Council will ensure appropriate contract clauses are in place

The Council will ensure that any contracts with third party data processors will have appropriate Data Protection, GDPR and record management clauses regarding the agreed and approved methods of information handling and storage and, if relevant, set out how information will be transferred back to the Council at the end of a contract.

6 GOVERNANCE, APPROVAL AND REVIEW

6.1 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.

6.2 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 Corporate Director of Resources, 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.

6.3 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 Information Governance Team who will feed back any issues to CGG.

Name	Role	Signature	Date Signed
Nicki Beardmore	Interim Corporate Director of Resources and SIRO		
Leila Ridley	Head of Information Governance and Data Protection Officer		
Peter Fehler	Acting Director of Law and Monitoring Officer		
Lisa Ford	Information Management Lead		
Jon Cumming	Interim Chief Information Officer		