



**Highland Council**

**Records Management Policy**

## Contents

1.	Document Control .....	3
1.1	Version History .....	3
1.2	Document Approval .....	3
2.	Introduction.....	4
3.	Definition of a Record .....	4
4.	Purpose and Scope .....	4
5.	Policy Statement.....	4
5.1	Records Management Processes and Record Keeping Systems.....	5
5.2	Principles of Good Records Management.....	5
5.3	Corporate Information Asset Register.....	6
5.4	Business Classification Scheme .....	7
5.5	Corporate Retention Schedules.....	7
6.	Records Management Governance .....	8
6.1	Information Management Governance Board (IMGB).....	8
7.	Roles and responsibilities .....	8
7.1	All Staff and any person handling Council Information.....	8
7.2	Managers and Supervisors.....	9
7.3	Information Asset Owners & System Owners.....	9
7.4	Information & Records Manager .....	10
7.5	Information Management Lead Officer .....	10
7.6	Information Management Link Officer .....	10
7.7	Internal Audit.....	11
8.	Legal Obligations.....	11
8.1	Public Records (Scotland) Act 2011.....	11
8.2	Data Protection Act 1998 .....	11
8.3	Freedom of Information (Scotland) Act 2002.....	11
8.4	Environmental Information (Scotland) Regulations 2004.....	12
9.	Related Policies.....	12
10.	Standards .....	12
11.	Staff Communication & Training .....	12
12.	Review .....	13

## 1. Document Control

### 1.1 Version History

Version	Date	Author	Change
v1	1997		Previous format that covered records management
v2	10/06/2009	Denis Torley	New Records Management Policy. Approved by Resources Committee
v3	09/10/2013	Philip Mallard, Alison Brown	1. Review and Restructuring 2. Addition of Document Control 3. Alignment with IM strategy and other IM Policy and updated to reflect changes in governance.
V3.1	25/02/2015	Philip Mallard, Trevor Nicol	Annual review of IM Policy Framework. Minor updates. Approved by Resources Committee
V3.4 DRAFT  (Version 4 when approved)	03/11/2016	Philip Mallard Information & Records Manager	IM Policy Framework Annual Review

### 1.2 Document Approval

Name	Role	Reason
	Resources Committee	Approval
Michelle Morris	Depute Chief Executive	Review and acceptance
	Information Management Governance Board (IMGB)	Review and acceptance
Vicki Nairn	Head of Digital Transformation	Review and acceptance

## **2. Introduction**

The Council's records are its corporate memory, supporting its core functions and providing evidence of actions and decisions. They are a vital corporate asset, enabling effective management and compliance with legal and regulatory obligations.

The Public Records (Scotland) Act 2011 and the Code of Practice on Records Management under Section 61 of the Freedom of Information (Scotland) Act 2002 both require the Council to have an effective records management policy in place. This must set out the legislative, regulatory and best practice framework within which we operate, and the way in which we aim to ensure our records remain accessible, authentic, reliable and useable through organisational or system change.

All records created and received by the Council in the course of its business are Council Information Assets owned by the Council and not by the individuals, teams, departments or services that create the records.

## **3. Definition of a Record**

The international Records Management Standard ISO 15489-1:2001 defines a record as "Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations, or in the transaction of business".

The Council recognises this as its definition of a record and that information includes all formats, whether paper or electronic e.g. hand written notes, letters, word documents, spreadsheets, scanned images, photographs, audio, emails, etc.

## **4. Purpose and Scope**

The Records Management Policy outlines the Council's commitment to the proper management of its records throughout their lifecycle from their creation through to their disposal, and defines the relevant roles and responsibilities for record keeping.

It defines the principles we follow when developing the Council's records management processes and record keeping systems.

The Policy applies to any person with access to Council records or any Council Information Asset. This includes staff, contractors, agency staff, members and those working on behalf of the Highland Council.

## **5. Policy Statement**

The Highland Council is committed to the creation of authentic, reliable and useable records and to their effective management throughout their lifecycle.

Records will accurately document the council's activities and support both operational needs and compliance with legislative and statutory obligations.

## 5.1 Records Management Processes and Record Keeping Systems

The Council's records management processes and record keeping systems shall be developed in order to:

- deliver consistency in the management of records across the Council;
- ensure that accurate and complete records are created that provide accountability and meet legal and business needs;
- ensure records containing personal and other sensitive information are stored according to the appropriate security classification and can only be accessed by authorised personnel;
- ensure that records can be promptly and efficiently retrieved with a clear audit trail maintained;
- avoid the accumulation of ephemeral material;
- ensure records keeping systems comply with the Council's Business Continuity Plan by identifying and preserving its vital records;
- ensure the Council's Corporate Retention Schedules and Disposal Authority processes are observed to ensure records are retained for the appropriate and agreed period of time;
- ensure records with long-term historical value are transferred to the custody of the Highland Archive Service for permanent preservation;
- ensure compliance with legal, audit and operational requirements affecting the retention of records, including the Public Records (Scotland) Act 2011, Data Protection Act, Freedom of Information (Scotland) Act and Environmental Information Regulations.

## 5.2 Principles of Good Records Management

The principles behind good record keeping require that:

- **Records are made** – Each service should have in place adequate arrangements for documenting its activities. These arrangements should take into account the legislative and regulatory environments within which it operates.

- **Records are accurate** – Records created are a correct reflection of what was done, communicated or decided.
- **Records are authentic** - An authentic record can be proven:
  - to be what it claims to be
  - to have been created or sent by the person claimed to have created or sent it
  - to have been created or sent at the time claimed

In order to ensure authenticity, records must be captured into a formal record keeping system which fits within the Corporate File Plan (filing structure) and includes the necessary metadata (i.e. data about data – a description).

- **Records are reliable** - A reliable record can be trusted as a full and accurate representation of the events, facts or activities to which it refers. Full records should be created at the time of, or as soon as possible after, the transaction or incident by individuals who have direct knowledge of the facts. Incomplete records can lead to decisions being made based on false assumptions and the evidential value is significantly diminished.
- **Records have integrity** – Records should be complete and unaltered. Any authorised annotation, addition or deletion should be explicitly indicated and traceable.
- **Records are usable** - A usable record can be located, retrieved, presented and interpreted. Records must still be usable even if the format the record is stored in is superseded or becomes obsolete. Electronic records should be migrated or transferred to new systems to insure against obsolescence.
- **Version control exists** – Where multiple versions of a record exist the current or official version should be identifiable.
- **Vital records are identified & protected** - Vital records are those which are crucial to the Council's business, without which the Council would be unable to function. These include records that, in the event of a disaster such as flood or fire would recreate the Council's legal and financial status, preserve its rights and ensure that it continued to fulfil its obligations to its stakeholders.

### 5.3 Corporate Information Asset Register

The Council's Corporate Information Asset Register is a key component of the Council's information architecture and an important part of effective records management. It defines the information that is held, provides details on the management of that information, and identifies Information Asset Owners and Information Asset Managers. This information is required to provide a single view of the Council's information holdings and support development of the information architecture to meet the needs for the management of this information. It also

provides information on the risk profile of the Information Assets, enabling prioritisation of resources to make information management improvements where this will deliver maximum value for the council. A council wide Corporate Information Asset Register has been created and a process in place for its maintenance.

An Information Asset is a collection of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles. Each ICT System and the information held within it is also considered to be an Information Asset.

The Corporate Information Asset Register provides Information Asset Owners with an overview of the information holdings that are within their scope of responsibility. Each Information Asset will contain records and it is the responsibility of the Information Asset Owner to ensure that there are appropriate records management processes and records keeping systems in place to manage those records. The approach taken to manage these records shall take account of the principles of good records management as set out in this policy.

Where there are weaknesses in records management processes or records keeping systems then these must be reviewed and plans put in place to address the weaknesses, taking into account the principles of good records management as set out in this policy.

#### **5.4 Business Classification Scheme**

A Business Classification Scheme creates structures for unstructured documents that have been identified as records, which can be used to create a corporate file plan or filing structure. We will establish a Highland Council Business Classification Scheme, which will take account of national standards and meet the requirements of the Public Records (Scotland) Act.

We will exploit the features of SharePoint 2010 to support the use of the Business Classification scheme where possible.

#### **5.5 Corporate Retention Schedules**

The Corporate Retention Schedules are the mechanism to ensure the Council is maintaining necessary records for the appropriate length of time. The Corporate Retention Schedules are made available to staff through the Intranet and are governed by the Information Management Governance Board.

The periods of retention for each type of record, the tools to manage the process of declaring a record and the disposal of it together form an important part of the Council's Information Architecture.

The retention periods set out in the Corporate Retention Schedules must be adhered

to by all Council Services.

## **6. Records Management Governance**

### **6.1 Information Management Governance Board (IMGB)**

The IMGB has been created to oversee the delivery of the Highland Council Information Management Strategy and govern the implementation of this across the Council. An IM Lead Officer from each of the Services represents their Service Director on the Board. Each Service Director is required to identify a member of their senior management team to act as IM Lead Officer for their service.

The IMGB is chaired by the Head of Digital Transformation as the corporate owner of Information Management Strategy and Policy and as Senior Information Risk owner (SIRO).

The primary role of the IMGB is to identify priorities for the implementation of Information Management improvements and the strategic initiatives identified in the IM Strategy Implementation Plan.

The IMGB has a duty to consider and make recommendations to the Executive Leadership Team about information management issues and influence strategy and policy development.

## **7. Roles and responsibilities**

This section sets out the general and specific responsibilities for Records Management.

### **7.1 All Staff and any person handling Council Information**

Records Management is everybody's responsibility and is something that should be considered as part of normal everyday working practice. This includes staff, contractors, suppliers, members and any person who handles Council Information Assets.

Staff and those handling Council information should understand the information that they create, receive and use and be able to identify information that is or may become a record. Records management processes that are in place must be followed and records keeping systems should be used in accordance with provided instructions and guidance.

Any person handling Highland Council Information must ensure that the records for which they are responsible are accurate and are created, maintained and disposed of in accordance with the Records Management Policy and the Corporate Retention Schedules.



All staff and those handling Council information must have completed the information management online learning module and any other relevant training that is required to use the records management systems and supporting ICT systems required in their role.

## **7.2 Managers and Supervisors**

Managers are responsible for information held within their area (both paper and electronic). This includes ensuring that an up to date and maintained list of Information Assets is held and that this is entered into the Corporate Information Asset Register.

Managers and supervisors must ensure that staff have understood their obligations under this Policy (both general obligations and those that are specific to their role) and other information management policies. Managers should support their staff in this regard by highlighting relevant parts of policies that apply to the roles being performed by a member of staff.

Managers and supervisors must ensure that all their staff have completed the information management online learning module and other relevant training.

## **7.3 Information Asset Owners & System Owners**

An Information Asset Owner (IAO) is a senior manager (head of service or equivalent) who has been identified as being accountable for a Highland Council Information Asset. A System Owner is a person who has been identified as being accountable for a Highland Council ICT System. The Information Asset Owner is supported by an Information Asset Manager (IAM), who has responsibility for management of the information within that Information Asset.

IAO and System Owners must ensure that the management of their Information Asset is consistent with the Records Management Policy and the other information management policies. The day to day responsibility for effective management of an Information Asset lies with the IAM. The IAO must ensure their IAMs are aware of their responsibilities.

IAO and System Owners must ensure that the information recorded in relation to their Information Asset in the Information Asset Register is correct and up-to-date.

The Corporate Information Asset Register contains a risk assessment for each Information Asset. The IAO must ensure that each IAM regularly reviews this risk assessment, and the RAG (Red, Amber, Green risk status) that is allocated to it. If the risk profile of the Information Asset changes then the IAM is required to inform the IAO.

Role descriptions for IAO and IAM have been developed and approved by IMGB. An online learning module has also been provided for Information Asset Owners and

Information Asset Managers that provides further explanation on their role and this must be completed.

#### **7.4 Information & Records Manager**

The Information & Records Manager is responsible for ensuring all Highland Council records are held within appropriate records management systems and structures. The Information & Records Manager is supported in this by the Records Manager and Records Management Service.

The Records Manager provides a Records Management Service to the council under a Service Delivery agreement between the Council and Highlife Highland. This includes the provision of advice on records management, the management of the council's Corporate Records Stores (including both paper records stores and the corporate electronic records store), and maintaining both the Council's Corporate Retention Schedules and Corporate Information Asset Register.

#### **7.5 Information Management Lead Officer**

The IM Lead Officer is a senior representative (head of service or equivalent) from each Council Service that represents their Service Director on the Information Management Governance Board (IMGB) and provides a strategic lead for information management issues (including records management) within each Service.

This includes a requirement to liaise directly with the Records Manager and the Information & Records Manager or to nominate representatives as the first point of contact for records keeping matters.

The IM Lead Officer will be required to attend the monthly IMGB meetings, communicate and cascade information within their Service and ensure adoption of working practices that are consistent with IM Policy and Guidance.

IM Lead Officers will be supported in their role through information and guidance provided through the Information Management Governance Board. Operational Support will also be available from IM Link Officers that have been identified within their service.

IM Lead Officers shall ensure that their service contributes to the development of and complies with the Corporate Retention Schedule and Disposal Authority process.

#### **7.6 Information Management Link Officer**

The IM Link Officer is a role that exists to provide support to the IM Lead Officer and the Corporate IM functions in the implementation of Information and Records Management.

## **7.7 Internal Audit**

The Highland Council's Internal Audit function includes responsibility for auditing the adequacy of the Council's Records Management Policy, procedures, internal records keeping systems, their implementation and Corporate and Service compliance with these.

## **8. Legal Obligations**

### **8.1 Public Records (Scotland) Act 2011**

The Public Records (Scotland) Act 2011 requires named public authorities in Scotland to prepare and implement a Records Management Plan (RMP). The plan must set out the proper arrangements for the management of the Council's records. Where authorities fail to meet their obligations under the Act, the Keeper has powers to undertake records management reviews and issue action notices for improvement. The Council RMP has been agreed with the Keeper

The Council is committed to ensuring a high level of performance of its records management processes and systems and therefore to incorporating regular reviews and assessments of its Records Management Plan. Ensuring all records management systems support business needs and comply with regulatory and accountability requirements will require regular review. Monitoring of the review will be conducted through the IMGB.

### **8.2 Data Protection Act 1998**

The Data Protection Act (DPA) regulates the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. It gives individuals a right of access to information held about them while protecting that information from third parties. The Act requires information to be accurate, up to date, retained for no longer than is necessary and protected against unauthorised access, loss, destruction or damage. The Information Commissioner has the power to investigate breaches and complaints in relation to DPA and to impose fines of up to £500,000 for non-compliance.

The Data Protection Policy provides further information on the Council's policy in relation to Data Protection Act compliance.

### **8.3 Freedom of Information (Scotland) Act 2002**

The Freedom of Information (Scotland) Act 2002 (FOISA) gives a general right of access to the information held by local authorities, giving the public the right to be told whether information exists and to receive that information (subject to certain exemptions) within twenty working days of making a request. Good records management will ensure The Highland Council is able to comply with this legislation.

## **8.4 Environmental Information (Scotland) Regulations 2004**

These Regulations give the public the right of access to information relating to the environment, which is held by local authorities. These requests can be made verbally, unlike requests made under FOISA which must be in writing. Good records management will ensure The Highland Council is able to comply with this legislation.

## **9. Related Policies**

This policy is complementary to and should be read in conjunction with the following

- Information Management Strategy
- Information Management Policy
- Records Retention and Disposal Policy
- Information Security Policy
- Data Protection Policy
- ICT Acceptable Use Policy

## **10. Standards**

The Council recognises the importance of using best practice and international standards in records management. It will therefore aim for compliance with the international standard for records management ISO 15489-1:2001 and the Code of Practice on Records Management issued under Section 61 of the Freedom of Information (Scotland) Act 2002.

## **11. Staff Communication & Training**

This policy will be made available to staff through the Intranet and for others who are within the scope of the policy through the Highland Council website.

As part of the core training, staff and any person handling Council information are provided with an online learning module that provides an introduction to the expectations the Council places on those handling information. This includes the records management as well as the information security and data protection issues of which all staff should be aware.

All staff must complete the information management online learning module and managers must ensure that this has been completed by their staff and is part of employee review and development.

Any other person handling Highland Council information must also complete this training and the relevant Information Asset Owners and Manager within the Council responsible for the contract must ensure this takes place.

Further online learning modules related to records management may be provided to staff and these must be completed where they are relevant to their role. Staff will be informed when they must complete these additional training modules. A specific online learning module has been provided and is mandatory for Information Asset Owners and Information Asset Managers.

## **12. Review**

This policy will be reviewed on a regular basis and adapted appropriately to ensure that it continues to meet the business and service delivery requirements of the Highland Council.