Highland Council

Information Management Policy

Contents

1. Document Control 3
1.1 Version History 3
1.2 Document Approval 3
2. Introduction 4
3. Purpose and Scope 4
4. Information Management Principles 4
4.1 Highland Council information is a corporate asset 4
4.2 Information Management is Everybody's Responsibility 5
4.3 We will manage information throughout its lifecycle 5
4.4 The right Information will be made available in the right place at the right time, accessible to those who need it. 6
4.5 We will ensure that information is accurate and fit for purpose 7
4.6 Information is re-used and shared where appropriate 7
4.7 Our ICT supports effective Information Management 8
5. Supporting Policies 9
6. Information Governance 9
6.1 Information Governance Board (IGB) 9
7. Roles and responsibilities 9
7.1 All Staff, and any person handling Council Information 9
7.2 Managers and Supervisors 10
7.3 Information Asset Owners & System Owners 10
7.4 Information Management Lead Officer 11
7.5 Internal Audit 11
8. Staff Communication & Training 11
9. Review 12

1. Document Control

1.1 Version History

Version	Date	Author	Change
V1	06/06/2011	Jennifer Boyle	Resources Committee Approval
V2	09/10/2013	Philip Mallard	Finance, Housing, Resources Committee Approval. Review and rewrite to reflect updated information management principles as set out in the IM Strategy and additional policy detail set out in reviewed Records Management Policy and new Information Security Policy.
V2.1	25/02/2015	Philip Mallard	Annual Review. Approved at Resources Committee.
V3	23/11/2016	Philip Mallard Information & Records Manager	Approved at Resources Committee. IM Policy Framework Annual Review
V4	18/10/2022	Miles Watters	Policy Framework Review Approved at Corporate Resources Committee 01/12/2022

1.2 Document Approval

Name	Title	Role
	Corporate Resources Committee	Approval
Kate Lackie	ECO Performance & Governance (Senior Information Risk Owner)	Review and acceptance
	Information Governance Board (IGB)	Review and acceptance

2. Introduction

The Information Management Policy supports the delivery of The Council's Information and Data Strategy and the Information Management Principles listed here are derived from that document.

It is part of the Information Governance Policy Framework that includes policies that also cover the detail of Records Management and Information Security.

3. Purpose and Scope

This policy applies to any person with access to Council records or any Council Information Asset. This includes staff, partners (such as High Life Highland), contractors, agency staff, members and those working on behalf of the Council.

The policy covers all the information the Council holds (Information Assets), regardless of its format (paper / electronic) or whether it was created within or outside the Council.

4. Information Management Principles

This policy sets out 7 Principles for the management of information and data in order to achieve our strategic aims:

- Council information is a corporate asset
- Information management is everybody's responsibility
- We will manage information throughout its lifecycle to ensure compliance with statutory and regulatory requirements, good practice and the Records Management Policy
- The right Information will be made available in the right place at the right time, accessible to those who need it
- We will ensure that information is accurate and fit for purpose
- Information is reused and shared where appropriate
- Our ICT supports effective information management

4.1 Highland Council information is a corporate asset

The culture and attitudes within the Council toward Information Assets will be such that information is seen as a valuable asset and accordingly treated with respect and professionalism without hesitation or second thought as the natural way to handle information.

We acknowledge that information is frequently created or received by individuals within the Council, and that the contribution of individuals is essential to achieving our business objectives, however, information as a resource is owned by the Council. In order to achieve its Business Intelligence Vision, the Council must be able to combine data across all functions.

Information, electronic and paper, and the systems used to create, access, use, store, manage and dispose of information will be treated as valuable corporate assets. Council Information Assets must not be used for any activity or purpose other than the Council's official business.

4.2 Information Management is Everybody's Responsibility

All staff and those handling Council information are personally responsible for the security and management of the information they create, capture, store and use.

Individuals are responsible for ensuring that the information they create or acquire is properly managed. Support in achieving this will be provided through information management guidance.

All Council staff who engage others to represent or work with the Council e.g. system suppliers, sub-contractors, consultants etc. are responsible for putting in place required controls and obligations in line with the Information Security & Assurance Policy and guidance.

Information Asset Owners will ensure that there will be regular briefings on Information Management and Security communicated to employees to ensure everybody knows their responsibilities for information management and security, including their responsibilities in managing contractors and relevant third parties. Support will be provided to Information Asset Owners through the Information Governance Board (IGB) and its board members (IM Lead Officers).

Further information on responsibilities is provided in section 7: Roles and responsibilities. The Records Management Policy and Information Security & Assurance Policy provide further detail on responsibilities for these areas of information management.

4.3 We will manage information throughout its lifecycle

We will manage information throughout its lifecycle to ensure compliance with statutory and regulatory requirements, good practice and Records Management Policy.

Wherever possible and appropriate, information will be stored in structured business systems. Unstructured Information will be stored in corporate repositories such as the Council network file shares and the Microsoft Office 365 platform, where it will be

managed in accordance with this policy, the Records Management Policy and supporting procedures.

Information will be labelled (using metadata) following Corporate guidelines to allow searching and retrieval of relevant information, and to understand the value and sensitivity of the information and its availability for use.

We will ensure that records are appropriately managed with professional records management that follows legislative requirements. Records management processes and records keeping systems will be developed to be consistent with the requirements of the Records Management Policy.

Information security controls, defined in the Information Security & Assurance Policy and the supporting Information Security Management System, will be applied to protect personal and other sensitive information in accordance with relevant legislation and Council policy.

The Council has an agreed security classification scheme and this scheme must be used where a security classification is applied to Council information (this is known as protective marking). The Council security classification scheme is consistent with the government security classification scheme, supporting appropriate sharing of information.

Protective marking shall be used where appropriate to highlight information that is sensitive to support appropriate handling of that information by recipients of the information both within the Council and by partners.

We will retain or dispose of information appropriately following the Records Management Policy and Corporate Retention Schedules. Information will be created, collected and stored as appropriate to the business need, and will be retained only for as long as it is needed to carry out its statutory functions, service provision and community obligations whilst having due regard to legislative and evidential requirements.

4.4 The right Information will be made available in the right place at the right time, accessible to those who need it.

Employees will benefit from appropriate information being readily available for them to undertake their duties effectively and efficiently. Information will be accessible anywhere and anytime with the correct access controls applied, regardless of where and how it is physically stored.

Information shall be created, stored and managed once for use many times, where the technology allows. Storing multiple copies of information reduces the ability to manage appropriately, and makes it more difficult to identify the correct version.

Links to information rather than attachments will be used in emails, where at all possible, to enable the preservation of “one version of the truth” and reduce storage space and the costs associated with it.

This will be supported through the use of corporate information repositories and tools such as the Council network file shares and the Microsoft Office 365 platform.

ICT Systems and paper stores will be designed to enable access to information to those people who need access as part of their role, but also ensure the access is appropriate and not excessive. There is a balance to be obtained where sufficient access to information is provided to enable people to carry out their role but not providing unnecessary access.

Having access to the wrong information can result in information overload or mislead, resulting in incorrect decisions and actions. Where this information is personal data, inappropriate access would be in breach of the Data Protection legislation and the Council could be subject to fines from the Information Commissioner's Office. Personal and sensitive or commercial information should also be controlled so that only those that need to see it can.

4.5 We will ensure that information is accurate and fit for purpose

Good data quality is a fundamental requirement to support the Council's Digital Strategy and the Business Intelligence Vision. Information Asset Owners must ensure the quality of the data collected and stored in their systems through standards and guidance which are clearly communicated to staff.

Employees will be able to trust in the accuracy and integrity of the information made available to them. They will be able to quickly and unambiguously identify the owner and the correct version of any piece of information held by the Council.

Information will be accurate and fit for purpose and the publishing process will be supported by a review and approval process to ensure consistent quality and appropriate content. Review dates will be applied for published electronic information.

Information will be presented in compliance with obligations to specific audiences, and will consider the Equality Act and the Council's Gaelic Language Plan.

4.6 Information is re-used and shared where appropriate

Information and data, once generated, will be available for re-use across the Council where appropriate, thus avoiding unnecessary duplication of effort. Re-use of data across the Council will enable the Council to derive benefits from good Business Intelligence.

This will support a learning organisation, with staff benefiting from the information products of others and avoiding re-invention and re-discovery. Readily accessible information combined with performance information will enable new and improved ways of working and support continuous improvement based on accurate and timely information.

Information sharing will support better decisions, and the ability to reuse information improves efficiency and effectiveness. Staff will make information they create or hold accessible, unless restricted by legislative and regulatory obligations, especially for personal and other sensitive information.

Staff are responsible for access to information they create or hold. Staff will manage information they create or hold in accordance with the sensitivity of that information. This may be identified through the Information Security Classification the information has been marked with. In the absence of a protective marking an assessment should be made by the recipient to decide the appropriate security classification of the document and handle it as appropriate to the sensitivity.

Information will be readily shareable, where appropriate between Services, functions, partners and third parties, enabling the delivery of consistent and joined-up services.

Data sharing involving personal data requires specific data sharing agreements and data processing agreements. Sharing of personal information with partner agencies is supported the Community Planning Partnership and the Highland Public Protection Chief Officers Group.

The Council will proactively make information available to the public through the Council website wherever this is appropriate. In addition the Council shall, where possible, make non-personal and non-commercially sensitive information available for external re-use. In particular, the Council shall work towards making its data open and available for re-use, in compliance with its obligations under the Re-use of Public Sector Information Regulations 2015 and the INSPIRE (Scotland) Regulations 2009.

4.7 Our ICT supports effective Information Management

Information Systems and use of technology must be secure, coordinated, compatible, integrated and supportive of Information Management policies and processes.

We will make assessments of Council computer systems against recognised standards for Information Security management, including ISO/IEC 27001 and CESG / PSN Government requirements, and where appropriate ensure compliance. The Information Security & Assurance Policy, supported by the more detailed Information Security Management System, sets out the security controls that ICT Systems must use.

The controls needed to ensure the protection and security of the Council's Information Assets will be determined by a process of risk assessment and analysis. A risk based approach is at the centre of the Council’s approach to information security and this ensures that investment is made in the most effective areas and risks eliminated or mitigated.

The Information and Data Strategy and ICT Strategy support achievement of this Information Management Principle.

5. Supporting Policies

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

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

6. Information Governance

6.1 Information Governance Board (IGB)

The IGB oversees the delivery of the Council's Information and Data Strategy and govern the implementation of this across the Council. There is an IM Lead Officer from each of the Services that will represent their Executive Chief Officer (ECO) on the Board. Each ECO is required to identify a member of their senior management team to act as IM Lead Officer for their Service.

The IGB is chaired by the ECO Performance & Governance as the corporate owner of the Information and Data Strategy, the Information Governance Policy Framework and as Senior Information Risk Owner (SIRO).

The primary role of the IGB is to identify priorities for the implementation of Information Governance improvements and the strategic initiatives identified in the Information and Data Strategy Implementation Plan.

The IGB has a duty to consider and make recommendations to the Executive Leadership Team about information governance issues and influence strategy and policy development. It also exists to support delivery of information governance improvements within services.

7. Roles and responsibilities

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

7.1 All Staff, and any person handling Council Information

Information Management is everybody's responsibility and is something that should be considered as a part of normal everyday working practice. This includes staff

(including all staff in schools), 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 and understand the security requirements. Information and records management processes that are in place must be followed and records keeping systems should be used in accordance with provided instructions and guidance.

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 (paper and electronic). This includes ensuring that an up to date and maintained list of Information Assets is held and that this has been entered into the Corporate Information Asset Register.

Managers and supervisors must ensure that all their staff have understood their obligations under this Policy (both general obligations and those that are specific to their role) and other Information Governance 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 is a senior manager (head of service or equivalent) who has been identified as being accountable for a Council Information Asset. A System Owner is a person who has been identified as being accountable for a Council ICT System. The Information Asset Owner is supported by an Information Asset Manager, who has responsibility for management of the information within that Information Asset.

Information Asset Owners and System Owners must ensure that the management of their Information is consistent with information governance policies.

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

Role descriptions for Information Asset Owners and Information Asset Managers 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 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 Governance Board (IGB) and provides a strategic lead for information governance issues (including records management) within each Service.

The IM Lead Officer is required to attend the IGB meetings, communicate and cascade information within their Service and ensure adoption of working practices that are consistent with Information Governance Policy and Guidance.

IM Lead Officers will be supported in their role through information and guidance provided through the IGB.

A Role description for the Information Management Lead Officer has been developed and approved by IMGB.

7.5 Internal Audit

The Highland Council's Internal Audit function includes responsibility for auditing the adequacy of the Council's Information Governance Policies, procedures, internal procedures, their implementation and corporate and Service compliance with these.

8. 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 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 Personal Development Plans. Alternative training may be undertaken where this is equivalent to the information management online learning module. It is the responsibility of managers to ensure that any training provides equivalent coverage and adequately covers Council policy.

Any other person handling Highland Council information must also complete this training or where otherwise instructed complete alternative training or read guidance that has been made available to them by the Council. The relevant Information Asset

Owner and Manager within the Council responsible for the contract must ensure this takes place, and that any alterative training or guidance is equivalent to the Council training.

9. 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.