Agenda Item	7
Report No	RES/30/22

THE HIGHLAND COUNCIL

Committee: **Corporate Resources Committee**

Date: **1 December 2022**

Report Title: **Information Governance Policy Framework**

Report By: **ECO Performance and Governance**

1. Purpose/Executive Summary

1.1 The report presents the review and update of the Council's Information Governance Policy Framework, highlighting the major changes which have been approved by the Council's Information Governance Board.

1.2 The Policy Framework is an essential part of the Council's compliance with the Public Records (Scotland) Act 2011 as well as being key to the compliance with the data protection legislation. The Policy Framework will be a key component of the Council's submission of its Records Management Plan to the Keeper of the Records in compliance with the 2011 Act.

2. Recommendations

2.1 Members are asked to:

- Approve the policies which make up the Information Governance Framework
- Agree that future updates to these policies are agreed by the Information Governance Board and will come back to Committee for approval where necessary.

3. Implications

3.1 Resource
There are no additional resource requirements. Management of information and records is embedded within each function of the Council.

3.2 Legal
Compliance with the access to information legislation is obligatory and failure to comply could result in legal action against the Council.

3.3 Community (Equality, Poverty, Rural and Island)
None

3.4 Climate Change / Carbon Clever
None

3.5 Risk
The Information Governance Policy framework is intended to reduce the Council's exposure to risks associated with lack of compliance e.g. data breaches or cyber attack.

3.6 Gaelic
None

4. Background

4.1 Corporate Resources Committee has recently approved strategies relating to Information and Data, ICT and Digital. The Information Governance Policy framework provides the foundations to support the successful implementation of these strategies by providing clear guidance about how Council staff should treat the information assets they work with.

4.2 The framework is made up of the following policies:

Data Protection Policy
Information Management Policy
Information Security and Assurance Policy
Records Management Policy
Records Retention and Disposal Policy

4.3 Each Policy has been approved by the Council's Information Governance Board (IGB) prior to being presented to the Corporate Resources Committee. Subject to approval, each policy will be reviewed annually by the IGB and will be reported to Committee where significant changes are required.

4.4 The responsibility for ensuring that this policy framework is complied with sits with the Council's Information Asset Owners. These are the senior staff responsible for systems and processes used to handle the Council's information and their role is set out within the policies.

4.5 Each Policy is presented as a separate appendix and the main changes are summarised below. They have all been updated to reflect the changes within the Council's Senior Management and Service structures and the Information Governance Board since their last review.

5. Data Protection Policy

5.1 The Data Protection Policy sets out the Council's intentions in relation to complying with the data protection legislation. It was redrafted in 2018 to take account of the EU General Data Protection Regulation and the Data Protection Act 2018. An appropriate

5.2 policy document is required by the Data Protection legislation when processing special category data under certain conditions.

5.3 The policy has been updated to reflect the fact that the UK is no longer a member of the EU. As a result, the GDPR no longer applies in the UK, it has been replaced with the UK GDPR which maintains the vast majority of the EU GDPR's obligations.

5.4 Changes have been made to the text of the policy in relation to data sharing (page 12) and international transfers (pages 10 and 13). The Highland Data Sharing Partnership was previously key to sharing information among partner organisations but this no longer exists and the text has been updated with a more general statement about data sharing agreements.

5.5 International transfers of personal data is an area which is greatly affected by the UK's exit from the EU. Adequacy agreements are required between countries to ensure that personal data can be transferred without difficulty. Prior to Brexit, the EU member states would not have been considered third countries in relation to international transfers of personal data, but this is no longer the case. As a result, the UK has agreed that it will continue to transfer personal data to the EU and the EU has published an adequacy decision regarding the UK's processing of personal data. However, the EU's decision will last until 2025 and may be revoked if the UK makes changes to data protection legislation which reduces the safeguards and standards of protection.

5.6 The situation in relation to adequacy agreements is subject to sudden change as was experienced when the EU struck down the "privacy shield" mechanism for adequacy arrangements with the USA. Such changes can expose the Council to risk in relation to the legality of data transfers and it is necessary to ensure that the location of our data is known and understood especially when moving to cloud based storage. These risks can be minimised by ensuring that our data is stored within the UK but this is not always possible. The text regarding Data Protection Impact Assessment (page 13) has been updated to reflect the importance of this issue.

6. Information Management Policy

6.1 The Information Management Policy sets out the principles for the management of the Council's information, regardless of format.

6.2 As with the Data Protection Policy, the Highland Data Sharing Partnership was key to sharing information among partner organisations at the time the previous version of the IM policy was drafted. The text under Section 4.6 has been updated with a more general statement around the Community Planning Partnership.

7. Information Security & Assurance Policy

7.1 The Information Security & Assurance Policy sets out the Council's management commitment and approach to ensuring the confidentiality, integrity and availability of its information.

7.2 Section 7.11 of the policy has been updated to take account of the move to hybrid working. The previous version of this policy referred to mobile and flexible working as an exception which required approval whereas the move the increased levels of hybrid

working means that is important that this does not lead to a reduction in information security.

7.3 A clear distinction is made between arrangements put in place to meet immediate emergency requirements (when staff have to vacate a building to work from home) and longer-term working arrangements. In emergency situations it may not be possible to fully assess and mitigate against security risks, but that assessment should be done as soon as practically possible and certainly if the arrangements become long-term.

7.4 Information Asset Owners are responsible for ensuring that risk assessments are carried out in relation to the processing of information that is taking place outwith Council buildings as a result of hybrid working.

8. Records Management Policy

8.1 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.

8.2 Under the 2011 Act, the Council must submit a records management plan for approval by the Keeper of the Records. The Keeper assesses the Council's arrangements against a number of elements related to information and records management (including the policies which are the subject of this report). The Keeper has added a new element 15 to his assessment which relates to records created by third parties on behalf of the Council and the scope (section 4) of the Records Management Policy has been updated to reflect this and to indicate the Council's commitment to element 15.

9. Records Retention and Disposal Policy

9.1 This Policy should be read in conjunction with the Records Management Policy. It outlines the Council's approach to managing the retention and secure disposal of information in line with business requirements and legal obligations and applies to all physical and digital information regardless of storage location.

9.2 An addition has been made under Section 5 relating to the destruction of records in-house and the maintenance of a disposal log for recording the disposal of all physical and digital records by Services.

Designation: ECO Performance and Governance

Date: 16 November 2022

Author: Freedom of Information and Data Protection Manager

Background papers

Appendices:

Appendix 1 – Data Protection Policy draft v2.1

Appendix 2 – Information Management Policy draft v4

Appendix 3 – Information Security and Assurance Policy draft v3

Appendix 4 – Records Management Policy draft v4.1

Appendix 5 – Records Retention & Disposal Policy v4

Highland Council
Data Protection Policy

Contents

Contents

1. Document Control

Version History

Version	Date	Author	Change
1	24/09/2013	Miles Watters	FHR Committee Approval
			Approved at FHR 09/10/2013
1.1	20/11/2013	Miles Watters	Amendment to 5.8 to add other areas recognised by EC. In recognition of Schedule 1, Part II Section 15 of the Act.
1.2	28/01/2015	Miles Watters	Annual review. Approved at Resource Committee 25/02/2015
1.3	07/04/2016	Miles Watters	Amendment of Sections 7 and 8 to reflect Internal Audit findings
2.0	17/04/2018	Miles Watters	Rewritten to reflect the requirements of the EU General Data Protection Regulation and the UK Data Protection Act 2018
2.1	31/05/2022	Miles Watters	Updated to reflect Brexit changes to data protection legislation

Document Authors

Miles Watters: Freedom of Information & Data Protection Manager

Distribution

Name	Role	Reason
	Resources Committee	Approval
	Information Governance Board	Review and acceptance
Kate Lackie	Executive Chief Officer, Performance & Governance and Senior Information Risk Owner	Review and acceptance

2. Introduction

The Highland Council is fully committed to compliance with the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA). The Council will take appropriate measures to ensure that all employees, elected members, contractors, agents, consultants and partners of the council who have access to any personal data, held by or on behalf of the Council, are fully aware of and abide by their duties and responsibilities under Data Protection Legislation.

3. Statement of policy and Scope

In order to operate efficiently, The Highland Council has to collect and use information about people with whom it works. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it is in paper or electronic format, and there are safeguards within the Data Protection Legislation to ensure this.

The Highland Council regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the Council and those with whom it carries out business. The Council will ensure that it treats personal information lawfully and correctly.

To this end the Council fully endorses and adheres to the Principles of Data Protection and to the principle of “Data Protection by design and default”.

This policy applies to all Highland Council employees, agents of the Council, persons representing the Council (including sub-contractors and consultants), Trade Union representatives and Elected Members.

4. Glossary of terms

Personal data

Personal data means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Special Categories of personal data

Special categories of personal data means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.

Processing

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection,

recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Conditions for processing
The legislation provides conditions for the processing of any personal data. It also provides separate conditions for processing "personal data" and "special categories of personal data".

Some processing of personal data carried out by certain parts of the Council, which carry out enforcement activities, are not subject to the UK GDPR. This processing comes under the definition of "law enforcement processing" is subject to Part 3 of the DPA. This affects Criminal Justice, Trading Standards, Environmental Health and Planning Enforcement.

Appendix 1 gives the conditions for processing as contained in Articles 6 and 9 of the UK GDPR and Section 31 of the DPA (Law enforcement purposes).

5. Handling of personal data

The legislation stipulates that anyone processing personal data must comply with six principles. These principles are legally enforceable.

The Highland Council will, through appropriate management and controls, adhere to the principles of data protection. The principles are listed below.

5.1 Principle 1 – Lawfulness, fairness and transparency

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject; [UK GDPR Article 5(1)(a); Section 35 of the DPA]

Staff must be aware of the reasons for which they process personal data and be able to explain this to the data subject. The Council has prepared privacy notices which will assist with this explanation and which state the conditions under which personal data is processed for a specific purpose.

Personal data may not be processed unless one of the conditions of Article 6, Article 9 or the Law Enforcement purpose applies (see appendix 1).

5.2 Principle 2 – Purpose limitation

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes; [UK GDPR Article 5(1)(b); Section 36 of the DPA]

Data subjects must be informed of all purposes for which their data will be used at the time of collection. Services must ensure that privacy notices contain clear explanations of how data will be used. Any use of personal data for statistical analysis shall be governed by these 6 principles.

5.3 Principle 3 – Data minimisation

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; [UK GDPR Article 5(1)(c); Section 37 of the DPA]

This means that the Council shall only collect the specific data necessary to complete a given task. It would be a breach of principle 3 to collect additional data.

5.4 Principle 4 – Accuracy

Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; [UK GDPR Article 5(1)(d); Section 38 of the DPA]

This depends on the nature of the data being processed. In some cases data will not change over time, whereas in other cases data will be updated on a regular basis. In all cases the Council must ensure the accuracy of the data being processed.

5.5 Principle 5 – Storage limitation

Personal data 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject; [UK GDPR Article 5(1)(e); Section 39 of the DPA]

All managers and staff will adhere to the Council's Records Management Policy and ensure that the Council's Corporate Retention Schedules are adhered to.

5.6 Principle 6 – Integrity and confidentiality

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures; [UK GDPR Article 5(1)(f); Section 40 of the DPA]

All managers and staff within the Council's Services will comply with the Council's information security and information management policies. They will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure, and in particular will ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
- Personal data held on computers and computer systems is protected by the use of secure passwords, which comply with the Council's password policy
- Personal data held on portable devices is encrypted.

5.7 Additional measures

In addition to adhering to the principles of Data Protection, The Highland Council will ensure that:

- A Data Protection Officer is appointed in compliance with Articles 37, to 39 of UK GDPR and Sections 69 to 71 of the DPA;
- Everyone managing and handling personal data understands that they are contractually responsible for following good data protection practice;
- Everyone managing and handling personal information is appropriately trained to do so;
- Everyone managing and handling personal information is appropriately supervised;
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;
- Queries about handling personal information are promptly and courteously dealt with;
- Methods of handling personal information are regularly assessed and evaluated;
- All projects and changes which affect the use of personal data will follow the principle of Data Protection by design and default;
- Regular and systematic data sharing is carried out under a written agreement as described below.

All elected members are to be made fully aware of this policy and of their duties and responsibilities under the legislation.

6. Data Subject Rights

Data Subjects have a number of rights under Data Protection Legislation:

- The right to be informed (UK GDPR Articles 13 & 14; DPA Section 44) (see section 7)
- The right of access (UK GDPR Article 15; DPA Section 45)
- The right to rectification (UK GDPR Article 16; DPA Section 46)
- The right to erasure (UK GDPR Article 17; DPA Section 47 & 48)
- The right to restrict processing (UK GDPR Article 18; DPA Section 47 & 48)
- The right to data portability (UK GDPR Article 20)
- The right to object (UK GDPR Article 21)
- Rights in relation to automated decision making and profiling (UK GDPR Article 22; DPA Section 49)

Each of these rights has a common set of standards which the Council must adhere to:

- Requests must be in writing but the Council must accept requests submitted by email or other electronic means.
- The Council may request identification to ensure that the information is provided to the right person.
- All requests must be responded to in one month (30 calendar days).

- Where the Council fails to respond in one month it must provide an explanation and inform the data subject of their right to contact the Information Commissioner's Office to complain.
- The response time can be extended by two months if the request is complex. The Council must inform the data subject of the extension within the first month and provide an explanation.
- Information must be provided free of charge unless the request has already been answered.
- The information provided in a response must be clear, concise and in plain English.
- The Council doesn't have to respond to requests that are considered "manifestly unfounded or excessive" and the Council can charge a reasonable fee to cover the costs of complying with these requests. In these cases the Council must provide an explanation which demonstrates that the request is unreasonable.

A full explanation of these rights and when they can and can't be accessed is given on the Council's website – www.highland.gov.uk/data-protection

A form is available on the Council's website to enable Data Subjects to submit requests and guidance for staff on how to deal with requests is available on the Council's intranet. Separate guidance on how to deal with access requests is also available to staff on the intranet.

All Data Subject requests will be recorded on the Council's Customer Relationship Management System to enable requests to be managed and to enable performance reporting.

7. The right to be informed

Unlike the other data subject rights, where the data subject must make a request in writing to the Council, the right to be informed is an obligation (under Articles 13 & 14 of UK GDPR and section 44 of the DPA) for the Council to provide information to data subjects at the time that personal data is first collected for a specific purpose.

This obligation is met through the provision of privacy notices specific to the purposes for which the Council processes personal data. A privacy notice must provide the following information:

- The identity and contact details of the Council (Data controller).
- Contact details for the Council's Data Protection Officer.
- A clear description of the purposes of the processing and the legal basis for carrying out the processing including which condition under Article 6(1) of UK GDPR applies.
- If the data is required for statutory reasons or in relation to a contract, the consequences of failing to provide the data must be provided.
- Whether the data will be shared and details of who the data will be shared with.
- Whether the data will be transferred to a 3rd Country (see section 8).
- The period for which the data will be stored.
- Details of the data subject rights which apply.
- If consent is the basis for processing, you must explain how to withdraw consent.

- Details of the right to complain to the ICO and contact details.
- Where data is processed automatically or used to create a profile of the data subject, details of this processing must be provided.

The Council's privacy notices are published on the Council's website.

8. Transfer to third Countries

Both the UK GDPR and the DPA put restrictions on the transfer of personal data to countries out with the UK ("third countries"). These restrictions are intended to ensure that the level of protection for personal data is not undermined by such transfers.

Transfers may take place to third countries which are the subject of "adequacy regulations" by the UK Government. Currently these countries and territories are Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Iceland, Norway, Liechtenstein, Gibraltar, Andorra, Argentina, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, Uruguay, Japan (only private sector organisations), and Canada (only covers data subject to Canada's Personal Information Protection and Electronic Documents Act).

Transfers may also take place where the recipient in the third country has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. Examples of appropriate safeguards are

- Standard clauses adopted by the UK Government
- Binding corporate rules
- Contract clauses authorised by the Information Commissioner

The issue of transfer to third countries has the greatest impact on the Council in relation to ICT contracts especially those involving cloud based services. Information Asset Owners must ensure either that the data warehouses or server farms (including mirrored sites and backup sites) which are used to store their data are located within the UK or a third country which is subject to an adequacy agreement.

If this is not the case then appropriate safeguards, as outlined above, must be put in place prior to the transfer of personal data. The advice of the Data Protection Officer should be sought in relation to such issues.

In particular circumstances, and only on a case by case basis, it is possible to use derogations or exemptions to transfer personal data to a third country. However, no such transfers should be made without first seeking the advice of the Data Protection Officer.

9. Data processing agreements

The Council may use third parties or contractors to carry out the processing of personal data on its behalf. This processing may only take place under the written instruction of the Council and must comply with Article 28 of the UK GDPR (Section 59 of the DPA).

Data processing agreements must meet the following criteria:

- The agreement must be in writing.
- The processor must be able to provide sufficient guarantees that they are able to implement appropriate technical and organisational measures to ensure the protection of the personal data being processed on the Council's behalf.
- The processor may not appoint any sub processor without authorisation from the Council and the Council must be informed of any intended changes in relation to sub processors.
- The processor must remain liable for any sub processor(s) and the sub processor must be subject to the same obligations as the processor
- The processor must only process personal data under documented instruction from the Council.
- The processor must not make any decisions about the purposes for which the personal data may be processed.
- The processor's staff which process personal data must be subject to an obligation of confidentiality.
- The processor must ensure the security of processing.
- The processor must assist the Council in relation to Data Subject rights requests.
- The processor must assist the Council in relation to security, breach notification and data protection impact assessments.
- The processor must provide assistance with demonstrating compliance with data protection legislation and must cooperate with audits and inspection by the Council or their appointed auditor.
- The agreement must describe how personal data will be transferred back to the Council at the end of the agreement and securely deleted by the processor, unless there are legal reasons for the processor retaining the data

The above terms may be included in the main contract or can be the subject of a separate data processing agreement.

10. Joint Controllers

In some circumstances, the Council and a partner organisation or contractor may consider that both parties are involved in making decisions about the processing of personal data. Where two or more controllers jointly determine the purposes and means of processing, they are known as joint controllers.

In such circumstances, the roles and responsibilities of all parties must be clearly documented and made available to data subjects, to give data subjects an understanding of how their personal data will be processed and by whom. It must be clear who the data subject should contact in each organisation to exercise their rights under the data protection legislation.

It must also be clear which party will fulfil the legislative requirements in relation to the provision of privacy notices to data subjects and these privacy notices should explain the joint controller relationship in a clear and transparent way.

11. Data Sharing

Data Protection legislation does not prohibit the sharing of personal data where it is appropriate. It may be appropriate to share personal data for a number of reasons including:

- There may be a legal requirement to share
- You may have received the consent of the data subject
- Sharing may be in the best interests of the data subject
- Sharing may be necessary to prevent or detect crime

It is the responsibility of Information Asset Owners to assess the nature of the relationship between the Council and other organisations (contractors, consultants, partners etc.) in terms of the control of personal data. This will enable them to decide whether they are joint controllers or whether a data sharing agreement or a data processing contract (see Section 9) is required in each specific case where personal data under the control of the Council is shared.

Where information is being shared either with a different organisation or internally, for a purpose other than that for which the data was collected, a data sharing agreement must be agreed. A data sharing agreement describes which condition for processing applies, the reason for sharing, the data to be shared and the key contacts in the organisations that the data is being shared with. It will also specify the purposes for which the shared information can be used.

Guidance on data sharing is available on the Council's intranet and the Information Commissioner's Office has produced a Code of Practice for Data Sharing.

The Highland Council has existing data sharing agreements in place with its key partner organisations such as NHS Highland, Police Scotland, The Scottish Fire and Rescue Service, Highlife Highland and the Scottish Government among others. Council staff must be familiar with any existing data sharing agreements which relate to their functions.

The Council will create and maintain a register of Data Sharing Agreements.

12. Data Protection Impact Assessments

Article 25 of the UK GDPR and Section 57 of the DPA place obligations on the Council to ensure that the protection of the rights and freedoms of data subjects is central to all processing of personal data. This is known as Data Protection by design and default. It requires the Council to ensure that all of its processing of personal data complies with each of the Data Protection Principles.

Data Protection Impact Assessments (DPIAs) are a useful tool to assist the Council with achieving this aim. The Information Commissioner has produced a handbook for DPIAs and guidance on carrying out these assessments is available on the Council's intranet. The Data Protection Officer will provide advice and guidance in relation to DPIAs.

The Council will carry out DPIAs in the following circumstances:

- New projects or initiatives

- Data protection Audits
- Where a mandatory DPIA is required by the legislation

12.1 DPIA for new projects

The Information Commissioner's Office advocates that the protection of privacy through good data protection practice should be built into processes right at the start rather than being considered towards the end of a project and then requiring expensive changes. This complies with the obligation for Data Protection by design and default.

A DPIA will be carried out prior to implementing new procedures or systems or making changes to existing procedures or systems. By considering privacy at the very start of a new initiative, the system or process can be designed to have least privacy impact and also be more efficient.

The Council will carry out a privacy impact assessment for any new projects or systems which use personal data or have the potential to affect privacy. Project Boards must ensure that the requirement for a DPIA is agreed at project initiation.

An important aspect of a DPIA for new systems is to understand where the personal data is being stored, especially in relation to cloud storage, and to ensure that this complies with the rules around international transfers described in Section 8 above.

12.2 DPIA in Data Protection audits

One of the statutory tasks of the Data Protection Officer is to monitor compliance with the Data Protection Legislation. This will be carried out through the use of DPIAs to assess whether current practices comply with the Data Protection principles.

12.3 Mandatory DPIAs

Article 35 of the UK GDPR and Section 64 of the DPA require the Council to carry out a mandatory DPIA where the type of processing envisaged is likely to result in a high risk to privacy. Nine types of processing have been identified which are likely to result in a high privacy risk and the ICO will also publish a list of processing operations which require a mandatory DPIA. The nine types of processing are:

- Evaluation or scoring
- Automated decision making with legal or similar significant effect
- Systematic monitoring
- Sensitive data or data of a highly personal nature
- Data processed on a large scale
- Matching or combing data sets
- Data concerning vulnerable data subjects
- Innovative use or applying new technology or organisational solutions
- When the processing, in itself, prevents data subjects from exercising a right or a contract

If an Information Asset Owner is considering carrying out processing which fits within one of these nine criteria they must first contact the Data Protection Officer for advice.

It is envisaged that in the majority of cases DPIAs will be published.

13. Breaches

Where a breach of data protection occurs, it is important that the Council takes immediate steps to reduce the impact on those whose data is affected. The Council must also report breaches to the Information Commissioner's Office within 72 hours of becoming aware of the breach, where the breach will result in harm to the rights and freedoms on data subjects.

All Security breaches must be reported to the ICT Service Desk (01463 253150) immediately. Where security breaches involve personal data, the Data Protection Officer must also be informed immediately. The Data Protection Officer may request that a data protection breach report is compiled. The breach report must provide details of the incident, how it occurred, steps taken to reduce the impact, steps taken to ensure that the same breach does not occur again and any lessons which should be shared within the Council to avoid similar incidents in other sections. The breach report must also include details about the numbers of people affected and the type of information involved.

Once completed, the breach report will be copied to the relevant Executive Chief Officer, as well as the Data Protection Officer. The Data Protection Officer is responsible for reporting the breach to the ICO and will usually provide a copy of the breach report.

If it is not possible to gather all the required information regarding a breach within the required 72 hours, the Data Protection Officer will contact the ICO to provide notification of the breach and inform them that further information is being gathered.

Staff with concerns around potential breaches of Data Protection should contact the Data Protection Officer for advice. Guidance on the breach procedure is available on the intranet.

14. Data Protection Fees

The Council is required by the Data Protection (Charges and Information) Regulations 2018 to pay an annual fee to the Information Commissioner's Office. The ICO has powers to serve monetary penalties on data controllers who refuse to pay the fee.

As well as the Council, the Highland Licensing Board is required to pay an annual fee. While all Councillors are considered to be data controllers in their own right, they are exempt from paying fees. The Data Protection Officer manages the payment of these fees.

15. Supporting Policies

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

Information and Data Strategy
Information Management Policy
Records Management Policy
Records Retention & Disposal Policy

Information Security & Assurance Policy
ICT Acceptable Use Policy

16. Roles and responsibilities

This section sets out the general and specific responsibilities for ensuring that the principles of Data Protection are adhered to.

16.1 All Staff, and any person working on behalf of the Council

Data Protection is everybody's responsibility and is something that should be considered as a part of normal everyday working practice.

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 record 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.

16.2 Managers and Supervisors

Managers are responsible for information held within their area. 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 all their 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. They should also ensure that staff are aware of any relevant data sharing agreements.

16.3 Information Asset Owners & System Owners

An Information Asset Owner is a person who has been identified as being responsible for a Highland Council Information Asset. A System Owner is a person who has been identified as being responsible for a Highland Council ICT System.

Information Asset Owners and System Owners must ensure that the management of their Information Asset is consistent with the principles of data protection and that the Council's Information Security & Assurance Policy is adhered to.

Information Asset Owners 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.

16.4 Senior Information Risk Owner (SIRO)

The SIRO is the senior person responsible for management of information security risks and for reporting this to the Executive Leadership Team. They are the corporate owner of the Information Governance strategies and policies The SIRO role is performed by the Executive Chief Officer, Performance and Governance.

16.5 Security Management

Information Security Incident Management and Investigations are managed by ICT Services on behalf of the Head of ICT and Digital Transformation.

16.6 Freedom of Information and Data Protection Manager

The FOI & DP 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.

The FOI & DP Manager, in conjunction with the Head of ICT and Digital Transformation, is also responsible for ensuring the Council's Information Security Management System, Information Management and Security Policies, and Information Security Incident Reporting processes support the Council's compliance with the Data Protection legislation.

16.7 Data Protection Officer

The Data Protection Officer is a statutory role which is set out in Articles 37 to 39 of the UK GDPR and Sections 69 to 71 of the DPA. Their tasks include:

- the provision of information and advice to Council managers and other staff in relation to the Data Protection legislation.
- monitoring the Council's compliance with data protection legislation and its own policies in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and related audits.
- the provision of advice in relation to data protection impact assessment and monitor the Council's compliance with the obligation to carry out mandatory DPIAs.
- acting as the contact point for the Information Commissioner's Office with regard to any matters relating to data protection.
- managing the process for dealing with requests all data subject rights requests
- providing advice and assistance to members of the public in relation to data protection

16.8 Responsible Premises Officer (RPO)

An RPO is responsible for the physical security of buildings through the effective management of perimeter security and zoning of buildings. Physical security of information within a business unit or building zone is the responsibility of the Information Asset Owners, individual managers and staff who work within those areas.

The RPO must respond promptly to any building physical security issues that are brought to their attention by any member of staff (or visitors) to remove or reduce any information security risk. Any remaining risk must be reported by the RPO to the Senior Information & Security Officer and the relevant Information Asset Owners / Managers. These staff must then report this through their management chain to their Service management team to be considered as part of the Highland Council's approach to risk management. A list of all properties and RPOs is maintained on the Council's intranet.

16.9 Information Governance Board (IGB)

The IGB has been created to oversee the management of The Highland Council Information Management Strategy and the implementation of this across the Council. The IGB is chaired by the Senior Information Risk Owner. There is an IM Lead Officer from each of the Services who will represent their Service 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 primary role of the IGB is to identify priorities for the implementation of Information Governance improvements and the strategic initiatives identified in the associated Strategies and Implementation Plans.

The IGB has a duty to consider and make recommendations to the Senior Management Team about information governance issues and influence strategy and policy development.

The work of the IGB in relation to information governance will ensure that the Council improves its Data Protection practice. Compliance with this Data Protection policy will be reported to the IGB.

16.10 Information Management Lead Officer

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

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.

16.11 Customer Resolution and Improvement Team

The Customer Resolution and Improvement Team is key to the coordination of Data Subject rights requests. They act as the contact point for Service staff and for the Data Protection Officer and provide assistance to Service staff in responding to requests.

16.12 Internal Audit

The Council's Internal Audit function includes responsibility for auditing the adequacy of the Council's Information Management policies, procedures, internal procedures, their implementation and Corporate and Service compliance with these.

17. Staff Communication & Training

This policy and associated guidance 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 (www.highland.gov.uk).

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 data protection as well as information security and records management issues that staff should be aware of.

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 their Employee Review & Development Plan.

Any other person handling Highland Council information must also complete this training. The relevant Information Asset Owners and Managers within the Council must ensure this takes place in relation to the data processing and contracts they have responsibility for.

18. 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 as well as changes to legislation.

Appendix 1 – Conditions for processing personal data.

UK GDPR Article 6 – Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

   a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; [Consent]

   b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; [Contract]

   c) processing is necessary for compliance with a legal obligation to which the controller is subject; [Legal obligation]

   d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; [Vital interests]

   e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; [Legal authority]

   f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. [Legitimate interests]

Point (f) shall not apply to processing carried out by public authorities in the performance of their tasks.

GDPR Article 9 – Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

   a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where domestic law provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject; [Explicit consent]

   b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised

by domestic law or a collective agreement pursuant to domestic law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; [Employment and social security]

c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; [Vital interests]

d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects; [Appropriate bodies]

e) processing relates to personal data which are manifestly made public by the data subject; [Published information]

f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; [Legal claims]

g) processing is necessary for reasons of substantial public interest, on the basis of domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; [Substantial public interest]

h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of domestic law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3; [Health and Social Care]

i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of domestic law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; [Public Health]

j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on domestic law (as supplemented by section 19 of the 2018 Act) which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. [Archiving and research]

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under

domestic law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under domestic law or rules established by national competent bodies.

3A. In paragraph 3, ‘national competent bodies’ means competent bodies of the United Kingdom or a part of the United Kingdom.

DPA 2018 Part 3, Section 31 – The law enforcement purposes

For the purposes of this Part, “the law enforcement purposes” are the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Highland Council

Information Management Policy

Contents

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

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.

Highland Council

Information Security & Assurance Policy

Contents

1. Document Control

1.1 Version History

Version	Date	Author	Change
V1	28/08/2013	Philip Mallard	Information Security Policy created and approved by FHR Committee.
V1.1	25/02/2015	Philip Mallard	IM Policy Framework Annual Review. Approved by Resources Committee.
V2	23/11/2016	Philip Mallard Information & Records Manager	Approved by Resources Committee. IM Policy Framework Annual Review Change to title from Information Security Policy to Information Security & Assurance Policy to better reflect scope. ICT Security Policy for Mobile & Flexible Working merged into Policy.
V3	17/10/2022	Miles Watters FOI & Data Protection Manager	Policy Framework Review

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 Security & Assurance Policy sets out the Council's management commitment and approach to ensuring the confidentiality, integrity and availability of its information.

It provides high level rules, responsibilities and roles that apply to members, staff, partners (such as High Life Highland), and those working on behalf of the Council or handling Council Information. The Information Security & Assurance Policy is part of the Information Governance Policy Framework, and together these set out the information security requirements.

More detailed operational requirements are set out in in the Council's Information Security Management System (ISMS).

3. Definition of Information Security

Information is an asset of the Council, and the Council needs to manage it as such, ensuring it is adequately protected. This is especially important in the increasingly interconnected and shared business environment.

Information can exist in many forms e.g. It can be printed or written on paper or stored electronically. Whatever form the information takes, or the means by which it is shared or stored, it should be appropriately protected.

Information security is the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to protect confidentiality, integrity and availability.

Information security is achieved by implementing a suitable set of controls, including the use of policies, processes, procedures, organisation structures, software and hardware. These controls need to be established, implemented, monitored, and reviewed (and where necessary improved), to ensure that the security and business objectives of the Council are met.

Information security requirements and the Data Protection legislation need not be a barrier to appropriate sharing of information. Through effective security controls and careful consideration of legal obligations we can be more confident in sharing information where appropriate.

4. Highland Council Commitment to Information Security

The Council is committed to effective Information Security through the management of information security risks that occur through both internal and contracted out activities.

The Council will implement and operate appropriate countermeasures and procedures to manage those risks down to an acceptable level, as determined by specialists within the Council, and in line with best practice.

The aim is to ensure business continuity, minimise business risks whilst maximising the return on investment and enabling business opportunities.

Through the Information and Data Strategy, supporting policies and the Information Governance Programme the Council will work to put in place the changes that are required to support the ISMS and effective information security.

The Council recognises that effective information security is achieved through a combination of policy, procedures, a risk based approach, security controls such as building security and most importantly staff information security awareness and skills. This requires an on-going commitment to continual improvement and change that can only be achieved through the support of all staff and those involved in handling Council Information Assets.

5. Policy, Legal & Standards Framework

The Council recognises that it works within a legal framework that places legal obligations on both the Council and its staff in relation to the management of information. The Council has an Information and Data Strategy and a framework of information governance policies that set out how we work to fulfil both the statutory obligations and our duty of care to people and organisations whose information we hold.

The legislation, policy and standards set out below are particularly relevant to the Information Security Policy, but there may be others that also have some relevance and the omission from this list in no way diminishes the Council's commitment to follow its obligations to comply with any statutory requirements and to work within best practice.

5.1 Council Information Governance Policy Framework

- Information Management Policy
- Records Management Policy
- Records Retention & Disposal Policy
- Information Security and Assurance Policy
- Data Protection Policy

5.2 Other relevant Council Policies

- ICT Acceptable Use Policy

5.3 External Standards

- ISO/IEC 27001/2 and ISO27000 Series

5.4 Legislation / regulation

- Data Protection Act 2018
- UK General Data Protection Regulation
- Computer Misuse Act 1990
- Regulation of Investigatory Powers Act 2000 (RIPA), Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) and other connected legislation.
- Copyright, Designs & Patent Act 1988 & other Intellectual Property Rights legislation
- Re-use of Public Sector Information Regulations 2015 and INSPIRE (Scotland) Regulations 2009

6. The Information Security Management System (ISMS)

The Councils approach to the management of Information Security is defined in the Information Security Management System (ISMS). This aims to coordinate and continuously improve the management of risk to information and sets out our approach to the application of our Information Security and Information Governance Policies. It commits the Council to design, implement and maintain a coherent set of policies, processes, and systems to manage risks to its information assets, thus ensuring acceptable levels of information security risk. The ISMS provides the means to understand risk, develops ways of managing that risk, monitors how effective that has been and identifies potential areas of improvement and how it needs to adapt to the changing business environment.

The Highland Council ISMS is based upon the international information security standard ISO/IEC 27001 and the implementation of the controls of ISO/IEC 27002. These standards are referred to as the “ISMS Family of Standards” and are recognised as the International de-facto Security Standards.

The ISMS will support management in ensuring that available security resources are spent on the areas that will deliver the greatest improvement in the management of information and reduction in risk e.g. are finances better invested in implementing additional security measures to the network or would investing in the security training of personnel be more effective?

The ISMS is supported by this Policy, and the other polices that make up the Information Governance Policy Framework. The Information and Data Strategy sets out the Council’s overall strategy for the management of its information which includes Information Security.

7. Information Security Policy Statements (in support of the ISMS)

The following are statements of Council Policy on issues that are important to the delivery of effective Information Security. The Council ISMS sets out operational details of how these are applied by the Council and further guidance will also be provided as appropriate to those affected by these policy requirements.

7.1 Encryption Policy - Cryptographic Controls and Key Management

Staff and any person working with Council Information Assets may only use encryption products that are authorised for use by ICT Services.

Only encryption products that include and make use of central key management should be used by the Council. Any exceptions to this must be approved by the Head of ICT & Digital Transformation and will require additional controls to be in place to ensure the encryption technology is appropriately managed. This must include (but not be limited to) the corporate retention of keys to enable decryption in the event of the Council being required to do so.

Technical controls and measures required for safe, secure and legally compliant use of encryption products will be maintained as part of the ISMS documentation and will be maintained by ICT Services.

The design and configuration of all Council ICT systems and those from third party providers used by the Council to store Council Information must adhere to this Encryption Policy and to the technical controls and measures that are set out as part of the ISMS. All contracts with providers and contractors must set out this requirement.

7.2 Physical / Building Security

It is the responsibility of the relevant Responsible Premises Officer (RPO) to ensure that a building used by the Council is adequately secure for the storage of the information that is held within it.

Managers and Information Asset Owners should ensure that any building they use for the storage of information (on paper or electronic storage) is adequate for the type of information they are holding. If there are any weaknesses in the building security then this must be reported to the RPO. Any other physical security issues such as a lack of local lockable storage must be dealt with by the Manager / Information Asset Owner responsible for that Information Asset.

7.3 Confidentiality Agreements & Data Sharing Agreements

Prior to any systematic, routine sharing of personal information there must be a data sharing agreement put in place. A copy of the data sharing agreement must be added to the Corporate Data Sharing Register.

Highland Council employment contracts will include confidentiality clauses.

Any third party that is provided with access to Council Information Assets must sign a confidentiality agreement that sets out their obligations and requires compliance with this Policy, ICT Acceptable Use Policy and all other relevant Council Policies (including those in the Information Governance Policy Framework).

7.4 Management of ICT Systems

All ICT systems must follow the requirements and controls set out in the Council ISMS and any supporting ISMS Policy documents. This should include but not be limited to the appropriate set up, management of systems, implementation and documentation of access controls.

All System Owners must ensure compliance with the Council ISMS and should create and maintain appropriate documentation to support management in accordance with the ISMS.

System Owners must be able to provide documentation as and when requested by ICT Services and Internal Audit that demonstrates their compliance with the ISMS.

7.5 Removable Media

Removable media is a data storage device that is not attached to a computer and can be used to hold and transfer information from one computer to another. This includes CDs, DVDs, Memory Sticks, Portable hard drives, memory cards (e.g. SD cards), and any electronic device that has internal storage (e.g. digital cameras and recording devices).

Removable media should only be used for the temporary storage and transportation of data. Where sensitive or personal data is being held on removable media the data and/or device must be encrypted and done so in accordance with the Encryption Policy (As set out in section 7.1). Handling of removable media must be appropriate to the type of information held on it and not be used to transfer Council information to personal devices as this use is contrary to this Policy and ICT Acceptable Use Policy.

Only removable media that has been approved for use by ICT Services may be used.

7.6 Disposal of Information held on ICT Equipment, Removable Media and Paper

All Computer media or paper that may contain personal or confidential data must be securely destroyed. Personal and Sensitive data must be removed from ICT equipment prior to destruction or recycling.

All ICT equipment and media must be disposed via an appropriate Council approved disposal service. This can be accessed by contacting the ICT Service Desk.

Paper containing personal or other confidential information must be disposed of using the Council confidential waste paper disposal bins or other approved method as defined in the Council's Confidential Paper Waste Procedure. If you do not have access to appropriate disposal services then you should contact your RPO to locate the nearest confidential waste paper disposal bin.

7.7 Clear Desk & Clear Screen Policy

All staff, those working on behalf of the Council, or handling Council Information must ensure that they lock their screen when computer equipment or mobile devices are left unattended and ensure that their screen cannot be read by others when they are in use.

All staff, those working on behalf of the Council, or handling Council Information must ensure that they leave their desk or working area clear of all personal or confidential information / documents when they are away from their desk (unless adequately managed on their behalf or the room is locked).

Laptops must be stored out of sight and not left out at the end of the working day. If possible, they should be stored in a locked cupboard or cabinet.

This section applies whether staff are working in a Council Building, when travelling on behalf of the Council or working from home.

7.8 Password Policy

System Owners must follow the ISMS Password Policy rules when defining requirements, and implementing systems.

Passwords used must be complex. The Council will ensure that any ICT systems use available technical controls to force complex passwords as appropriate to the information being held within the system.

All ICT users must ensure that they follow Council password guidance to create a complex password for each ICT System they access.

Passwords must be treated as confidential and not shared with others. Intentional sharing of passwords is a breach of the ICT Acceptable Use Policy.

If a password does become known to another person or there is a suspicion that a password has been compromised then this must be reported as a security incident by contacting the ICT Service Desk.

7.9 Intellectual Property Rights (IPR)

The Council will respect Intellectual Property Rights when handling information, working to ensure it complies with its legal obligations.

The Council's own IPR will be protected, whilst supporting re-use where appropriate. The Information Management Policy sets out the principle that Information will be reused and shared where appropriate. This includes allowing re-use both internally and externally of information that is non-personal and non-commercially sensitive. 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 INSPIRE (Scotland) Regulations 2009.

7.10 Vulnerability Assessment and Penetration Testing

The Council will carry out Vulnerability Assessment and Penetration Testing on its network infrastructure.

The Council will risk assess the need to carry out penetration testing and vulnerability assessment on its ICT Systems. It is the responsibility of each System Owner to assess the need for this based on the type of system and the information held within it.

7.11 Hybrid working

All handling and storage of Council electronic information must be done using ICT that has been authorised for this purpose. This requirement is further expanded in the ICT Acceptable Use Policy. Generally that will mean ICT equipment provided and managed by the Council's ICT Services team. However, some access to certain resources, such as M365 and Assure, is also made available for staff to access on personal devices. This is more limited and with higher levels of protection than for Council-supplied equipment. For instance, multi-factor authentication is likely to be mandated for such access.

All handling and storage of paper based Council information must be in accordance with this Policy, the Information Governance Policy Framework policies and local procedures. Paper based Council information must only be removed from Council premises where this has been authorised and appropriate arrangements are in place to protect the confidentiality, integrity and availability of this information.

Business processes that require information and ICT (that provides access to Council information) to be removed from Council premises shall be risk assessed to ensure security arrangements are adequate for the type of information. It is the responsibility of the relevant Information Asset Owner and Information Asset Manager to ensure that local procedures are produced and are communicated to those handling the information. A clear distinction is made between arrangements

put in place to meet immediate emergency requirements (when staff have to vacate a building to work from home) and longer-term working arrangements. In emergency situations it may not be possible to fully assess and mitigate against security risks, but that assessment should be done as soon as practically possible and certainly if the arrangements become long-term.

Local information handling procedures must be appropriate to the type of information being processed as part of the local business activity. These must include the following controls to protect information:

- Paper based Council information and Council ICT must be kept in sight at all times and be under the control of the Council representative when off site (subject to the exception where the Council is supporting a customer in completing information where the customer is the owner of the information).
- Use of Council ICT must be positioned in a way that complies with the clear screen policy (Section 7.7) and ICT Acceptable Use Policy to prevent unauthorised access to information. This should not prevent appropriate viewing of information by third parties where this is required as part of the business process.
- Council ICT and paper information must not be left in a car unattended during offsite working activity unless this is securely stored (not visible such as in a covered area in the boot of the car).
- Council ICT and paper information must not be left unattended in a car overnight. Exceptions may be made where this is the best possible security available, but in any case the information / ICT must not be visible and a risk assessment must be carried out.
- The Council's clear screen and clear desk policies, detailed in Section 7.7, must be complied with when working from home. Council ICT and paper information must not be left unattended and must be kept secure when not in use.
- Staff working from home must ensure meetings take place in a location where confidential discussions cannot be overheard by third parties.

Authorisation for Council staff to work from home or other locations not within Council Buildings must be captured within the New Ways of Working (NWOW) Teams Agreements. An appropriate information risk assessment must be carried out to understand the risks associated with these arrangements and this must be taken into consideration as part of the decision on whether to allow the hybrid working. Authority for mobile and flexible working shall be in line with the Council Flexible Working Policy.

NWOW Team Agreements should also capture the details of situations where Council information (e.g. paper file) or Council ICT devices that are not specifically designed for mobile use (e.g. Desktop PC) have been removed from Council premised by any person with permission from the relevant Information Asset Manager.

For third parties, such as contractors, any mobile and flexible working must be in accordance with contractual arrangements. It is the responsibility of Council staff to

ensure that these contracts require full compliance with this Policy and all other Council policies.

Any potential information risks associated with the location being used must be declared to the relevant Information Asset Manager at the earliest opportunity. One such risk would be sharing a working location with non-Council staff.

Particular attention must be paid to:

- the policy requirements for Clear Desk and Clear Screen (as set out in section 7.7) to ensure that information is not inadvertently disclosed through others being able to see information on paper and ICT equipment when out of the office.
- the requirements for secure disposal of Council information (as set out in section 7.6), which required that any paper held off site that requires secure disposal must be brought back for disposal using Council provided facilities.
- The requirements around the use of removable media (as set out in section 7.5), ensuring that only Council ICT is used to process Council information, information is not transferred to personal devices and Removable media is only used for the temporary storage and transportation of data.

7.12 Security Classification & Protective Marking

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.

8. Information Security Management Roles & Responsibilities

This section sets out the general and specific responsibilities for information security management, including reporting of information security incidents.

8.1 All Staff and any person working on behalf of the Council

Information Security is everybody's responsibility and is something that should be considered as part of normal everyday working practice. This policy and other policies in the Information Governance Policy Framework set out the information security requirements to be followed by staff at all levels, and further support is provided to staff through guidance and training where necessary.

All those working within a Council Building or handling Council Information anywhere must ensure that they observe the Clear Desk & Clear Screen Policy as set out in this Policy (section 7.7).

If a potential security issue or incident is identified then this must be reported by the individual or delegated nominee to the ICT Service Desk. This requirement is set out in the ICT Acceptable Use Policy, but this also applies equally to any security issue or incident that involves paper based information or physical security where this could impact on the security of Council Information Assets.

Any remote or mobile working that may involve information handling must be consistent with the requirements as set out in section 7.11 of this policy.

8.2 Managers and Supervisors

Security of information within a business unit or building zone is the responsibility of individual managers and staff who work within those areas.

Managers are responsible for information held within their area. This includes ensuring that the information is held securely, access controls are appropriate and maintaining an accurate and up-to-date a list of Information Assets in the Corporate Information Asset Register.

Managers must promptly report any building physical security issues to the Responsible Premises Officer. The RPO will work with appropriate staff to remove or reduce any information security risk. Managers must report any remaining risks, after risk reduction, through their management chain to their service management team to be considered as part of the Councils approach to risk management.

Managers and supervisors must ensure that all their staff have completed the Information Management online learning module and have understood their obligations under this Policy 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 their work area and that of their staff is adequately secured including the implementation of the Clear Screen and Clear Desk Policy as set out within this Policy (section 7.7).

8.3 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 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 (IAM), who has responsibility for management of the information within that Information Asset.

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. All Information Assets should be recorded in the Corporate Information Asset Register.

Each ICT system and the information held within it is also considered to be an Information Asset and is recorded as such in the Corporate Information Asset Register.

IAO and System Owners are responsible for ensuring that the security controls applied to their Information are appropriate and that it is held securely with access to the information being provided as appropriate.

IAO 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 and an accompanying online learning module for IAO and IAM have been developed and approved by IGB. These provide further explanation on the roles and all IAO / IAM must read the role description and undertake the online learning.

8.4 Senior Information Risk Owner (SIRO)

The SIRO is the senior manager responsible for management of information security risks and for reporting this to the Council's Executive Leadership Team. The SIRO role is performed by the ECO Performance & Governance.

The ECO Performance & Governance is the corporate strategic owner of Information Security as part of Information and Data Strategy.

8.5 Freedom of Information & Data Protection Manager

The FOI and DP Manager has operational strategic ownership of Council Information Assurance and Records Management on behalf of the ECO Performance and Governance.

The FOI and DP Manager is responsible for ensuring an operational records management service is in place. The Council Records Management Service is provided by High Life Highland under a service delivery agreement. This service includes the maintenance of the Corporate Information Asset Register, which contains information on the security classification and security controls of Information Assets.

8.6 Head of ICT & Digital Transformation

The Head of ICT & Digital Transformation is responsible for ensuring an operational security management function is in place. Information Security Incident Management

and Investigations are managed by ICT Services on behalf of the Head of ICT & Digital Transformation.

8.7 Data Protection Officer

The Data Protection Officer role is performed by the Freedom of Information & Data Protection Manager who is responsible for providing advice about compliance with the Data Protection legislation, for monitoring Privacy Impact Assessment and for reporting Data Protection Breaches to the Information Commissioners Office (ICO).

The Head of ICT & Digital Transformation is responsible for ensuring the Council's ISMS; Information Management and Security Policies, and Information Security Incident Reporting processes support the Council's compliance with the Data Protection legislation.

8.8 Responsible Premises Officer (RPO)

The RPO is responsible for the physical security of buildings through the effective management of perimeter security and zoning of buildings. Physical security of information within a business unit or building zone is the responsibility of the Information Asset Owners, individual managers and staff who work within those areas.

The RPO must respond promptly to any building physical security issues that are brought to their attention by any member of staff (or visitors) to remove or reduce any information security risk. Any remaining risk must be reported by the RPO to the relevant Information Asset Owners / Managers and Data Protection Officer. These managers must then report this through their management chain to their service management team to be considered as part of the Council's approach to risk management.

8.9 Internal Audit

The Council's Internal Audit function includes responsibility for auditing the adequacy of the Council's Information Security Policy, procedures, internal information security controls, their implementation and Corporate and Service compliance with these.

8.10 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 and Information Security within each Service.

The IM Lead Officer will be 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 IGB.

9. Information Security Governance and Process

9.1 Information Governance Board (IGB)

The IGB has been created to oversee the delivery of the Council Information and Data Strategy and govern the implementation of this across the Council. An IM Lead Officer from each of the Services represents their Service's 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 Information and Data Strategy and the Information Governance Policy Framework and as 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.

The IGB will review high level information security risks in support of the SIRO.

9.2 ICT Security Management

Operational ICT Security management is managed by ICT Services and will operate under Service management governance and the Head of ICT & Digital Transformation will report back to the IGB, identifying information risks that require consideration by the IGB. Any technical issues that are ICT Security risks or require ICT changes to manage the risk, will be referred to the appropriate board, following normal ICT Services service management governance.

9.3 Information Security Incident Reporting

Information Security Incidents or concerns about information security must be reported by staff through the ICT Service Desk.

The ICT Acceptable Use Policy sets out the Council's expectations on all ICT Users to report all security incident or concerns. This obligation also applies to any other

user of Council information or those working on behalf of the Council when this concerns paper based information.

9.4 Information Security Incident Management Procedure

The ICT Acceptable Use Policy sets out the monitoring that the Council may undertake of ICT usage. The Council may produce Potential Misuse Reports on the activity of a user or investigate any information security incident, regardless of whether the incident involves information held in ICT systems or on paper. The procedure is set out in more detail in the ICT Acceptable Use Policy.

10. Staff Communication & Training

This policy and other information governance policies are made available to staff through the Intranet and others within scope of the policies through the Council website.

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 information security and data protection issues that staff should be aware of.

All staff must complete the Information Management online learning module and managers must ensure that this has been completed by their staff.

Any other person handling Council information must also complete this training and the relevant Information Asset Owners and the Council manager responsible for the contract, involving third party handling of information, must ensure this takes place.

Further information security online learning modules 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.

11. 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.

Highland Council

Records Management Policy

Contents

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
V4	23/11/2016	Philip Mallard Information & Records Manager	Approved by Resources Committee IM Policy Framework Annual Review
V4.1		Miles Watters FOI & Data Protection Manager	IM Policy Framework Review

1.2 Document Approval

Name	Role	Reason
	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 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 15489-1:2016 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, video, 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, elected members and those working on behalf of the Highland Council.

The Policy also applies to records created by, or on behalf of, a contractor carrying out the Council's functions.

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 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 risk assessment 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 legislation, Freedom of Information (Scotland) Act 2002 and Environmental Information (Scotland) Regulations 2004.

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 is 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. A Highland Council Business Classification Scheme will be established which will take account of national standards and meet the requirements of the Public Records (Scotland) Act 2011.

Microsoft Office 365 will be used 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 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 Governance Board (IGB)

The IGB has been created to oversee the governance of the processing and management of information within the Highland Council. Each Executive Chief Officer (ECO) is required to identify a member of their senior management team to act as the representative for their Service.

The IGB is chaired by the ECO, Performance and Governance as the corporate owner of the Council's information governance policies and strategies and as the Senior Information Risk Owner (SIRO) for the Council.

The primary role of the IGB is to identify priorities for the implementation of Information Management improvements and strategic initiatives across the Council.

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

Where required, the IGB will appoint relevant staff to an Information Governance Working Group to work on specific tasks and make recommendations on its behalf.

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, Elected 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. They should 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 instructions and guidance provided by line management.

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.

The Information Management Portal details the roles and responsibilities of staff who manage Council information. It provides specific and useful information on managing records, managing emails, working securely; and exploiting the use of SharePoint, OneDrive and MS Teams in order to carry this out effectively. Emphasis is placed on the importance of managing and protecting the information used in their work, particularly for those staff handling personal and sensitive information.

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, Strategic Lead 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 Freedom of Information and Data Protection Manager

The FOI & DP 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 the Council's Corporate Retention Schedules.

7.5 Information Governance Lead Officer

The Information Governance Lead Officer is a senior representative (Head of Service, Strategic Lead, or equivalent) from each Council Service that represents their ECO on the Information Governance Board (IGB) 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 FOI & DP Manager or to nominate representatives as the first point of contact for records keeping matters.

The IG Lead Officer will be required to attend the regular IGB meetings, communicate and cascade information within their Service and ensure adoption of working practices that are consistent with Information Governance Policies and Guidance.

IG Lead Officers will be supported in their role through information and guidance provided through the Information Governance Board and the Information Governance Working Group.

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 Local Records Officers

The Local Records Officers (LROs) are appointed by Services to provide a link between the Service and Records Management. The LRO is the conduit through which all records requests, both transfers and retrievals, are channelled. The RM Service only fulfils records requests submitted by the relevant LRO for that area.

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 IGB.

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

The Data Protection legislation 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 legislation 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 Data Protection and to impose fines for non-compliance.

The Data Protection Policy provides further information on the Council's policy in relation to Data Protection 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 that 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 15489-1:2016 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.

Highland Council

Records Retention & Disposal Policy

Contents

1. Document Control

1.1 Version History

Version	Date	Author	Change
V1	18/08/2010	Susan Beckley, Highland Council Archivist	Approved by Resources Committee
V2	28/05/2014	Philip Mallard, Senior Information & Security Officer, Trevor Nicol, Records Manager	New approach to focus on defining retention periods in thecorporate retention schedules and making the disposal process more effective and efficient. Approved by Resources Committee.
V2.1	25/02/2015	Philip Mallard, Senior Information & Security Officer	Annual IM Policy Framework Review. Policy renamed from 'Records Retention Policy & Disposal Authority' to 'Records Retention& Disposal Policy'. Approved by Resources Committee.
V3	23/11/2016	Philip Mallard Information & Records Manager	Approved by Resources Committee IM Policy Framework AnnualReview Update relating to records heldon behalf of third parties.
V4		Miles Watters, FOI and Data Protection Manager, Trevor Nicol, Records Manager	Update relating to changes in Council's senior management and Service structure

1.2 Document Approval

Name	Title	Role
	Corporate Resources Committee	Approval
Kate Lackie	Executive Chief Officer (ECO) of Performance and Governance & SIRO	Review and acceptance
	Information Governance Board (IGB)	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.

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

The Council's Records Management Policy supports compliance with the Public Records (Scotland) Act 2011, the Code of Practice on Records Management under Section 61 of the Freedom of Information (Scotland) Act 2002, and the storage limitation principle under Data Protection Legislation.

Effective records management requires the management of records throughout their lifecycle from creation to disposal. The Records Retention and Disposal Policy sets out the Council's approach to the retention and disposal of its records.

3. Purpose and Scope

This Records Retention and Disposal Policy is part of the Information Management Policy Framework and supports the Records Management Policy through setting out the roles and responsibilities of Information Asset Owners and supporting staff in making record retention and disposal decisions.

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

4. Related Policies

This policy is complementary to and should be read in conjunction with the following policies that make up the Information Management Policy Framework

- Records Management Policy
- Information Management Policy
- Data Protection Policy
- Information Security & Assurance Policy

5. Policy Statement

The Council will ensure that records and information are not kept for longer than is necessary to carry out its statutory functions, service provision and community obligations, whilst having due regard for legislative and evidential requirements.

5.1 Definition of a Record

The Records Management Policy sets out the Council's agreed definition of a record:

"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 International Records Management Standard ISO 15489-1:2016)

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, video, etc.

5.2 Records Management Processes and Record Keeping Systems

The Council's Records Management Policy sets a range of council commitments in relation to its records management processes and record keeping systems. The following commitments are particularly relevant to the Records Retention and Disposal Policy:

- deliver consistency in the management of records across the Council;
- ensure records keeping systems comply with the Council's Business Continuity Plan by preserving its vital records identified in the Council's Corporate Retention Schedules;
- ensure the Council's 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 Legislation, Freedom of Information (Scotland) Act and EnvironmentalInformation Regulations.

5.3 Corporate Retention Schedules

A corporate retention schedule is the mechanism to ensure the Council is maintaining necessary records for the appropriate length of time. It determines the length of time records are required to be kept and provides the authority for disposal.

The Corporate Retention Schedules are an active management document designed to reflect the record types used by the Council and are subject to continual monitoring and review. They promote greater control over the Council's records, enabling Managers to dispose of records no longer needed, and ensuring the retention of appropriate records consistent with effective service delivery and the Council's legal and regulatory obligations.

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 followed by all Council Services, subject to the Disposal Authority Process set out in section 5.7 of this policy. The Highland Council Corporate Retention Schedules are available for consultation by staff on the council intranet.

5.4 Setting the Corporate Retention Schedules' Retention Periods

In setting the retention periods for the Corporate Retention Schedules, the Council will consider the following factors.

Legislation / Regulations

- Is there any legislation or regulation affecting retention of the records?
- Is the type of information likely to be required for conducting legal proceedings in the event of legal action being taken by, or against the Council? Time limits for commencing litigation can be found in the Prescription and Limitation (Scotland) Act 1973.
- Identify any particular regulatory agencies or statutes that may govern the business process generating the records.
- Identify any past/anticipated issues facing the Council from a litigation, regulatory or compliance perspective.

Operational / Business Need

- How long are the records likely to be needed to carry out the Council's functions?
- How long are the records required for evidential purposes in respect of business processes or decision making?
- How long do the records need to be kept for accountability/internal audit purposes?
- How serious would the consequences be if they were no longer available?

Ownership of records

- Are the records owned by the Council or are they being managed by the

Council on behalf of another organisation? For example NHS records being processed as part of integrated Health and Social Care.

- For records managed on behalf of another organisation, are retention periods being set by that organisation? If so these must be followed, particularly when this information contains personal data (these retention periods should be incorporated into the Council Corporate Retention schedules).
- Are there particular arrangements for the disposal of records managed on behalf of another organisation? Should they be returned to the owning organisation? Should they be destroyed using particular methods? Are there requirements for historical archiving and has the process been agreed with the external organisation?
- Are records created by, or on behalf of, a contractor carrying out the Council's functions retained in compliance with this policy?

Archival Value

- Do the records have long term historical value? If so it may be appropriate to transfer them to the Highland Archive Centre.
- Do the records document the Council's policies, structures and processes so that its activities may be understood by future generations?

Risk Assessment / Data Protection and Freedom of Information Legislation

- What are the risks involved in keeping these records?
- Will they be liable for disclosure under the Data Protection or Freedom of Information (Scotland) Acts, incurring costs of processing?
- If they contain personal data, have they served the purpose for which they were created?

Relationship with other records

- Are the records needed in order to understand or use other records? The retention periods of related records should be co-ordinated.

Open data and Re-use

- Is the record a dataset that has established use, either within the organisation, or outside?
- Would the destruction of a dataset that has been made available as open data impact on current re-use and therefore could there be business impacts or impacts on services to the highlands as a result?

Financial / Resource

- Can the records be retained for a shorter period to achieve savings in storage

and management costs, whilst still maintaining compliance with this policy and the Records Management Policy?

5.5 Reviewing the Corporate Retention Schedules' Retention Periods

Where an Information Asset Owner identifies a business or legal reason for retention period to be changed, this must be brought to the attention of the Records Manager and a review will be carried out in accordance with the process set out below:

1) The Records Manager will review the case for a change and seek further information on the justification for the change.

2) If there is a legal basis for a retention period then this will be referred to Legal Services to provide advice.

3) If the retention period is based on best practice then this will be considered by the Records Manager and a recommendation produced. The recommendation will be based on the factors set out in section 5.4.

4) The advice from both the Records Manager and Legal Services, combined with the business case for change from the service will be provided to the Information Governance Board (IGB). The IGB will review the information provided to them and take further advice from the Records Manager and Freedom of Information & Data Protection Manager.

5) The IGB will make a decision on the change and the Corporate Retention Schedules will be updated with immediate effect.

6) If a decision cannot be made due to the level of risk or where there is disagreement amongst IG Lead Officers then this will be referred to the Executive Leadership Team for final consideration.

5.6 Retention and Disposal Decisions

The Information Asset Owner responsible for a group of records is accountable and responsible for authorising the disposal of records. The authority to approve disposal actions may be delegated to a nominated person such as an Information Asset Manager (who has day to day responsibility for the management of the information). In the event of the decision being delegated then the Information Asset Owner (IAO) will remain accountable for that decision.

Retention and Disposal decisions must follow the retention periods as set out in the Corporate Retention Schedules, unless the disposal authority process as set out below requires a period of further retention. If the records under consideration for disposal are not clearly identified in the Corporate Retention Schedules then advice must be sought from the Records Manager. If there is a gap in the Corporate Retention Schedules then the review process set out in section 5.5 must be followed in order to create an additional entry. No disposal of records must take place unless there is an appropriate entry in the Corporate Retention Schedules.

It is also important to consider whether documents are the Council record or whether they are a copy. Copies of documents where the Council record is held by another part of the Council should be destroyed as soon as the business requirement for them has ended. As these documents are not considered to be a record then the retention of them is not governed by the Corporate Retention Schedules. The Information Asset Owner must confirm which department holds the definitive versions/originals to ensure an appropriate decision is taken.

The Corporate Retention Schedules set out the action that must be taken once a retention period has expired.

Disposal actions can be:

- Historic Archive
- Destroy
- Review
- External Transfer

5.7 Disposal Authority Process

Prior to any disposal of Council records the following steps must be undertaken.

1) **Review of outstanding Requests**

   At the end of a record's retention period the Information Asset Owner or delegated representative must ensure that there are no outstanding requests for information involving that record. In particular the IAO must consider whether any of the following requests have been received by the Council.
   a. FOI request
   b. Subject Access Request
   c. Legal Disclosure request

2) **Pending Legal Action Review**

   In addition to the above the IAO must assess if the documents are expected to be relevant to a pending legal case. In this case legal advice should be sought to ensure that the retention beyond the period set out in the Corporate Retention Schedules is appropriate. All documents that are required for legal proceedings should be kept until the threat of proceedings has passed.

3) **Final Review**

   The Information asset owner should consider if there is an overwhelming operational / business need to retain the records beyond the retention period identified in the Corporate Retention Schedules. In this event, advice must be sought from the Records Manager and records may only be retained with the

approval of the Information Governance Board.

4) **Disposal**

Where there are no such outstanding requests the record(s) can be disposed of with the approval of the IAO or delegated representative:

- **Where the disposal action is to 'Historic Archive':**

  The Information Asset Owner or delegated representative (or the Records Manager where the record is in RM custody) must arrange for the Archivist to review the record.

- **Where the disposal action is to 'Destroy':**

  The records, regardless of format must be destroyed or deleted. Any destruction must be done securely and follow Council's Information Security Policy and staff guidance on confidential waste destruction. Paper records can be destroyed in-house if a crosscut shredder is available, otherwise the Council's confidential waste contract should be utilised.

- Records in RM custody due for destruction should be uplifted and destroyed by the Council's confidential waste contractor.

- A disposal log must be maintained for all records destroyed or deleted in accordance with the corporate retention schedules and be retained permanently by the relevant Service.

- **Where the disposal action is to 'Review':**

  The Information Asset Owner should consider if there is an operational / business need to retain the records for a further period. Advice must be sought from the Records Manager.

- **Where the disposal action is "External Transfer":**

  The Information Asset Owner must arrange for the external transfer to the organisation as per the instructions in the Corporate Retention Schedules and in accordance with the agreements with the third-party organisation on whose behalf the Council is managing the records.

5) **Recording the Disposal**

The disposal action must be recorded in a Disposal Log.

5.8 Exceptions to the Disposal Authority Process (Automated Destruction)

The only exception to the Disposal Authority Process is where it has been agreed by

the Information Asset Owner and the Freedom of Information & Data Protection Manager that an automated process may be used to destroy electronic records.

Automated destruction of records shall only be approved where there are technical controls available to place a hold on the record or group of records to prevent the automated destruction of these records.

Where automated destruction of electronic records is in place the Information Asset Owner must ensure they have processes in place to instigate a hold on records to prevent destruction when the council becomes aware that a request has been received for records that may be automatically destroyed or where the council requires the records as per stage 1 to 3 of the Disposal Authority Process.

6. Records Retention and Disposal Governance

6.1 Information Governance Board (IGB)

The IGB has been created to oversee the governance of the processing and management of information within the Highland Council. Each Executive Chief Officer (ECO) is required to identify a member of their senior management team to act as the representative for their Service.

The IGB is chaired by the ECO, Performance and Governance as the corporate owner of the Council's information governance policies and strategies and as the Senior Information Risk Owner (SIRO) for the Council.

The primary role of the IGB is to identify priorities for the implementation of Information Management improvements and strategic initiatives across the Council.

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

The IGB is responsible for the approval of changes to the Corporate Retention Schedules and for approving exceptions in the event of an overwhelming operational / business need. It is also responsible for the approval of records management guidance and processes to support delivery of the Records Management Policy and Records Retention and Disposal Policy.

7. Roles and responsibilities

This section sets out the responsibilities for Records Retention and Disposal.

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 record 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 this policy, the Records Management Policy and the Corporate Retention Schedules.

Records must not be disposed of unless this has been approved by the Information Asset Owner and is in accordance with the retention period as set out in the current Corporate Retention Schedules.

The inappropriate destruction or deletion of records may result in the Council being unable to prove that it has or has not acted in a particular way. This may, for example, have financial repercussions or leave the Council unable to prove its case in a court of law. The destruction of a record that is the subject of an on-going request for information is likely to result in the loss of trust in the Council, and leave it open to criticism from members of the public and the media. Furthermore, under Section 65 of the Freedom of Information (Scotland) Act 2002, any member of staff who alters, erases or conceals records with the intention of preventing them from being disclosed, could be found guilty of a criminal offence which carries a maximum fine of £5000.

7.2 Managers and Supervisors

Managers are responsible for information held within their area (both paper and electronic).

Managers and supervisors must ensure that their staff have understood their obligations under this Policy 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 Records are not disposed of unless this has been approved by the Information Asset Owner, follows the Disposal Authority Process and is in accordance with the retention period as set out in the current Corporate Retention Schedules.

7.3 Information Asset Owners & System Owners

An Information Asset Owner (IAO) is a senior manager (head of service strategic lead 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 Highland Council ICT System. The IAO 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 this policy, the Records Management Policy and the other information management policies.

IAO and System Owners must ensure they comply with this policy when making a decision on the disposal of Council records.

Role descriptions for IAO and IAM have been developed and approved by IGB. 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 by them.

7.4 Freedom of Information & Data Protection Manager

The FOI & DP Manager is responsible for ensuring all Highland Council records are held within appropriate records management systems and structures. The FOI & DP 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 High Life 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 Highland Archive Service Digital Repository) and maintaining both the Council's Corporate Retention Schedules and Corporate Information Asset Register.

The Records Manager supports compliance with this policy by maintaining the Corporate Retention Schedules, providing effective records management guidance to IAO and IAM and ensuring records in its custody are disposed of in accordance with this Policy.

7.5 Information Governance Lead Officer

The IG Lead Officer is a senior representative (head of service strategic lead or equivalent) for each Council Service that represents their ECO on the IGB 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 record keeping matters.

IG Lead Officers shall ensure that their service contributes to the development of and complies with the Corporate Retention Schedules and Disposal Authority Process.

7.6 Local Records Officers

The Local Records Officers (LROs) are appointed by Services to provide a link between the Service and Records Management. The LRO is the conduit through which all records requests, both transfers and retrievals, are channelled. The RM Service only fulfils records requests submitted by the relevant LRO for that area.

7.7 Legal Services

Legal Services advise on whether retention periods are prescribed by law and to ensure that corporate interests are met through the appropriate retention periods being set in the Corporate Retention Schedules.

Advice will be provided to the IGB as required to support it in its role.

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 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.

The Information Management Portal details the roles and responsibilities of staff who manage Council information. It provides specific and useful information on managing records, managing emails, working securely; and exploiting the use of SharePoint,

OneDrive and MS Teams in order to carry this out effectively. Emphasis is placed on the importance of managing and protecting the information used in their work, particularly for those staff handling personal and sensitive information.

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.