Information Security Policy

Version 4.0, 03 May 2023

This is a controlled document. The digital PDF file published on InsideNL is the control copy.

- Always access this document from the control location.
- When you open this document, your device may automatically download it. If it does, you should still open it from the control location in future.
- You can print this document, but a printed copy isn’t the control copy.
- Don’t save any digital copies of this document anywhere. This includes your device, USB flash drives, network drives, OneDrive, Teams/SharePoint, or any other digital storage device, system, service, or location.

Document control

Title	Information Security Policy		
Governance group	Data Governance Board		
Owner	Katrina Hassell, Senior Information Risk Officer	**Contact**	hassellk@northlan.gov.uk
Author	Rob Leitch, Information Risk Manager	**Contact**	leitchro@northlan.gov.uk

Revision history

Version	Originator	Review start date	Revision description and record of change
4.0	Julie Irwine	03 May 2023	Biennial review and plain English changes.
3.0	Rob Leitch	09 March 2021	Review with aim of deprecating Information Risk and Information Classification and Handling policies.
2.1	Charles Muir	18 February 2021	Reviewed as part of review of all information governance policies and guidelines.
2.0	Rob Leitch	28 April 2020	Regular review including comments from Data Governance Board and Data Management Team.

Document approvals

Version	Governance group	Date approved	Date approval to be requested (if document still in draft)
4.0	Policy and Strategy Committee		08 June 2023
3.0	Policy and Strategy Committee	03 June 2021	
2.0	Policy and Strategy Committee	11 June 2020	
1.3	Policy and Resources Committee	21 June 2017	
1.2	Policy and Resources Committee	16 September 2014	
1.1	Policy and Resources Committee	14 March 2013	

Consultation record (for most recent update)

Consultation status	Stakeholders consulted between 15 March 2023 and 12 April 2023.	
Stakeholders consulted and dates	Business and Digital Management Team Data Management Team Data Governance Group Technical Design Authority	21 March 2023 15 March 2023 29 March 2023 21 March 2023

Strategic alignment

Plan for North Lanarkshire

Improving the Council’s Resource Base – A Workforce Strategy that is built around the needs of the council (as a single resource base) to deliver the priority outcomes, ensuring future workforce requirements, new skills and innovative approaches, and succession planning are recognised.

Digital and IT Strategy

The Digital and IT Strategy brings together separate but related plans and policies that contribute to the development and delivery of our digital vision. The Information Security Policy is one of these. It supports the strategy by providing a safe framework for using our information, and our information storage facilities and processing systems without exposing the council or our users to risks.

Next review date

Review Date	

Contents

A note about plain English

This document follows plain English guidance, in line with our corporate commitment to clear communications. In particular, it uses the following terms.

- 'We', 'us' and 'our' when referring to the council (as an organisation), our collective responsibilities (as authorised users of council IT assets), and when discussing specific activities.
- 'You' and 'your' when referring to the individual responsibilities and actions of authorised users of council IT assets.

1. Introduction

Information is a critical asset. We rely on physical assets and information technology (IT) to use, store, manage, process, and share information. We must secure and protect these so we can continue to deliver our services, carry out our statutory duties, and support our internal business functions.

Information security covers the following.

1. **Physical access** to electronic and paper-based information assets.
2. **Logical access to electronic information, and IT systems and services**, both hosted within our own network and cloud-based – including business systems and applications, office software, databases, websites, and apps.
3. **Network infrastructure and services** including hardware and software, both within our own network and through cloud managed services – including routers, switches, gateways, firewalls, servers, and monitoring and management tools.
4. **Legislation** governing data and IT systems, both corporate and business function specific.
5. **Compliance requirements and standards** set out by government and regulatory bodies.
6. **Privacy rights** of our customers, service users, employees and other authorised IT users.
7. **Supply chain security**, particularly where a third party holds our information or processes it on our behalf.

The council owns all information we store. We securely manage this along with the devices, systems and services we use to create, store, access and process it.

2. Purpose

This Information Security Policy provides a framework for effective information security that balances the benefits and risks of processing information. It is a control factor for the Information Security and Governance corporate risk and aligns with the following.

- Digital and IT Strategy – this brings together separate but related plans and policies – including this one – that contribute to our digital vision.
- Its sister policies – Data Protection , Payment Card Data Security, and Records and Information Management – that maintain the safety, confidentiality, integrity and availability of our information.
- Acceptable Use of IT Policy – this informs the council's IT users on how to appropriately use IT assets to store and process information.
- Related legislation.

3. Scope

This policy applies to every person who creates, accesses, processes and otherwise uses information on our behalf or in an official capacity – both IT and non-IT users. This includes all employees, councillors, contractors, consultants, temporary agency staff, modern apprentices, students, volunteers, and any other authorised third parties.

4. Governance

The **Policy and Strategy Committee** has **approval** authority for, and oversight of, this policy. The **Data Management Team** then the **Data Governance Board** – as **key stakeholders** – oversee its review and consider its contents before referring it on for approval. The **Chief Officer of Business and Digital** – as the council's Senior Information Risk Owner – is **accountable** for its governance. The **Information Security and Risk team** is **responsible** for the following activities.

1. Produce, publish and promote this policy.
   a. Write it in a way that's easy to read and understand.
   b. Consult with relevant stakeholders on its content and implications.
   c. Make sure all users can access it.
2. Give guidance on how to apply and comply with this policy through standards, procedures and guidance notes – see product set for list and links.
3. Review and report on this policy.
   a. Review every two years, with other reviews when needed. For example, following a critical security incident, new legislation, a significant threat, an audit action.
   b. Report to management teams, governance and working groups, committees and scrutiny panels.

5. Policy compliance

Every person with access to our information and who uses it in the course of council-related work or in an official capacity, must comply with this policy, and all the policies, standards, procedures and guidance it references.

This includes:

- only using our information for its intended purpose – unless authorised to do otherwise;
- maintaining its confidentiality and integrity, and
- keeping it safe.

Appendix 1 describes the roles and responsibilities of the following key people and groups in supporting, promoting and complying with this policy.

- Chief Executive
- Senior Information Risk Owner
- Corporate Management Team
- Business and Digital Delivery Board
- Data Governance Board
- Data Management Team
- Information Risk Manager
- All Managers
- Everyone in the scope of this policy.

6. Policy objectives

This policy sets our strategic position and lays the foundations for effective information security.

Its key objectives are as follow.

1. Show clear executive-level understanding of the value of information and the need to make resources available to protect it.
2. Help everyone who accesses or processes our information understand:
    a. why we must protect its confidentiality, integrity, and availability;
    b. the controls we use to protect it; and
    c. their role in this.
3. Show our key stakeholders – such as elected members, our residents, customers and service users – that we treat and protect information in line with its value and sensitivity.
4. Provide a development and review process for information security related standards, procedures, and guidance.
5. Promote compliance with all legislation and regulations governing our information assets.
6. Maximise the benefits of our information whilst identifying and managing associated information risks.

7. Information security controls

7.1. Managing risk

Managing risk is critical to keeping our information secure. This process includes identifying, assessing, and monitoring risks to

- the information we hold, and
- information storage facilities and processing systems.

We do the following to manage information risks.

1. Use network controls, specialist systems and privileged utility programs to protect our IT infrastructure.
2. Produce and promote policies, standards, and guidance.
3. Develop and implement security operational procedures.
4. Produce mandatory training for employees and deliver awareness sessions for councillors.
5. Routinely raise awareness about information security, both generally and topic specific. This includes issuing alerts and guidance about specific threats, as they occur.
6. Agree specific treatment plans for the risks we manage – and invoke them when we need to – in line with the Risk Management Strategy.

7.2. Managing information

This policy – and related Data Protection and Records and Information Management policies – define how we manage and use information. We have a range of supporting products, relating to specific elements of this. In particular –

Information classification and handling: The Standard and Guidance helps everyone:

- understand the different classes of information and what we use them for;
- decide which classification to use for an information asset, based on the sensitivity and confidentiality of its content;
- know how to handle information based on its classification.

Records retention: The Records Retention Schedule helps us decide

1. how long to keep information, and
2. whether to dispose of, archive or permanently preserve it.

Information assets: The Information Asset Register details all of our current information assets held on record. It includes the following for each:

→ asset reference, name and description;
→ owner, administrator, service and business unit;
→ classification and whether it contains personal information;
→ any legislative basis for processing the information; and
→ format (paper or digital) and reuse status.

Other guidance to help manage information securely.

We store user guidance on our InsideNL document library, covering specific topics including the following.

- Email security guidance
- Home Working and Information Security Guidance
- IT Authentication (Password) and Secure Access User Guidance

7.3. Training and awareness

We use training and awareness to help manage information risk. This includes giving people the knowledge and confidence they need to carry out their information security responsibilities. This in turn will change behaviours to further protect the information we hold, and our information storage facilities and processing systems.

There are a series of **mandatory training modules** on LearnNL covering the core elements of information governance.

- Data protection
- Information security
- Records and Information management

Employees must complete this training every two years to keep up to date with any changes in policy or legislation.

We carry out a range of **awareness raising activities** using different types of media and systems to promote information security, share information and build knowledge. We generally communicate with everyone but also target specific audiences – where appropriate.

Awareness raising

Activities

We maintain a constant flow of content to keep everyone involved and informed. Examples include the following.

- Routinely sharing information, both general and topic specific.
- Promoting events and campaigns such as Cyber Security Week.
- Publishing Cyber-i, the information security and risk quarterly digest.
- Issuing alerts and guidance about specific threats, as they occur – for example a new phishing scam designed to steal information.
- Engaging directly on Viva Engage (also known as Yammer), including answering questions, asking for opinions, and signposting to useful content elsewhere.
- Notifying users of policy changes, new standards, procedures and guidance.
- Delivering councillor awareness sessions.

Media

We use a range of media, including the following.

- Information Security and Risk community on Viva Engage
- Council news on InsideNL
- InsideNL Information Security and Risk document libraries
- Staff announcement emails
- Chief Executive’s newsletter
- Toast popup notifications
- PowerPoint presentations

7.4. Operational security

Information is at the core of all our operational activities. As such we use procedures and controls to manage it securely it at every stage of its lifecycle.

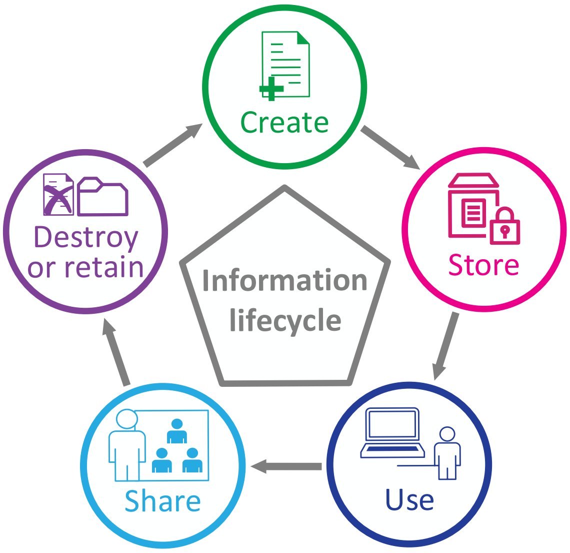

Figure 1: Information lifecycle

Key operational activities include the following.

- **Compliance:** Legislation, regulations, and data sharing arrangements.
- **People resources procedures**: Recruitment, disclosure and other vetting processes.
- **Access control**: How we control access to information and systems, as defined in our Access Control Standard, related procedures and guidance, and Code of Connection procedures. This comprises the following.
  - **User access** including identity and access management, provisioning, privileged access management, passwords and other authenticators, and user authentication and secure access responsibilities.
  - **Device access** including council devices and personal devices.
  - **Access to IT systems and services** including system controls to protect against unauthorised access, service disruption, data breach and data loss.
  - **Access to network infrastructure and services** including network controls and procedures, and privileged utility programs.
  - **Access to electronic information** using permissions and privileges.
- **IT operational controls:** This includes products and procedures to manage change, protect and manage our network infrastructure, introduce and decommission systems, and replace and dispose of hardware.
- **Information security incidents:** The Information Security Incident Management Procedure explains how we react to actual and suspected security incidents.
- **Business continuity:** The IT Systems Resiliency and Disaster Recovery Standard classifies IT systems in terms of how critical they are to our service delivery and business continuity. The most important systems are gold, followed by silver then bronze.
- **Supply chain security:** Following the Supply Chain Cyber Security Standard and Purchasing Cloud-based Services Cyber Security Guidance when buying cloud-based systems or services.

- **Procurement:** The Corporate Procurement model includes governance arrangements, procedures for engaging with suppliers, and procurement toolkits and templates.
- **Project management controls:** The Project Management Framework includes records management, data protection and information security guidance for its product set

8. Product set

The table below lists documents in the Information Security Policy product set and other related products. This may include links to other file types, websites and IT systems.

- Those listed under policies, standards, procedures and guidance are the responsibility of the Information Security and Risk team.
- Those listed under related products are the responsibility of other teams, services or agencies.

Product type	Product
Policies	▪ Acceptable Use of IT Policy ▪ Payment Card Data Security Policy
Standards	▪ Access Control Standard ▪ IT Systems Resiliency and Disaster Recovery Standard ▪ Information Classification and Handling Standard ▪ Supply Chain Cyber Security Standard
Procedures	▪ Access Control procedures ▪ Code of Connection procedures ▪ Information Security Incident Management Procedure
Guidance	▪ Cyber-i ▪ Email security guidance ▪ Home Working and Information Security Guidance ▪ IT Authentication (Password) and Secure Access User Guidance ▪ Information Classification and Handling Guidance ▪ Information Security and Risk on Viva Engage (aka Yammer) ▪ InsideNL document library ▪ Purchasing Cloud-based Services Cyber Security Guidance
	▪ Corporate Procurement model ▪ Council news on InsideNL ▪ Data Protection Policy ▪ Digital and IT Strategy ▪ Information Asset Register ▪ LearnNL ▪ Project Management Framework ▪ Records and Information Management Policy

Product type	Product
Related products (continued)	▪ Records Retention Schedule ▪ Risk Management Strategy
Legislation, regulations, and government guidance	▪ Data Protection Act 2018 ▪ Government Security Classifications ▪ Public Bodies (Joint Working) (Scotland) Act 2014 ▪ Public Records (Scotland) Act 2011 ▪ Scottish Public Sector Cyber Resilience Framework ▪ The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020

Appendix 1: Information security roles and responsibilities

Role	Responsibilities
Chief Executive of North Lanarkshire Council.	▪ Overall accountability for the protection of information we own and process.
Senior Information Risk Owner (SIRO) The Chief Officer of Business and Digital has this role.	▪ Make sure we protect our: ▪ information; and ▪ information storage facilities and processing systems. ▪ Accountable for information security governance.
Corporate Management Team The council's executive board. Members are the Chief Executive, Depute Chief Executive, SIRO, and Chief Officers.	▪ Sign off on our information security controls and practices. ▪ Consider reports on the effectiveness of our information security practices.
Data Governance Board A senior officer group of business information owners and subject matter experts from all services. Chaired by the SIRO.	▪ Assure robust information governance of this policy. ▪ Consider revisions before passing to the Policy and Strategy Committee for approval.
Data Management Team An officer group from all services with responsibility for business information including processes and IT systems.	▪ Individual members must make sure their service complies with this policy and related standards, procedures and guidance. ▪ Collectively the team: ▪ oversees the review of this policy; and ▪ agrees revisions before passing to the Data Governance Board for consideration.
Information Risk Manager Our lead subject matter expert on information security and risk management.	▪ Co-ordinate and monitor activities to manage our information risk posture, including: ▪ network controls, specialist systems, and privileged utility programs to protect our IT infrastructure; and ▪ mandatory training and awareness raising. ▪ Produce and promote this policy and related standards, procedures and guidance.

Role	Responsibilities
All managers Anyone responsible for managing a function or group of people within the council. This includes information owners.	- Make sure processes and security controls are in place to manage information effectively. - Make sure staff members: - follow policies, standards, procedures and guidance; and - keep up to date with mandatory training.
Everyone As per the scope, every person who creates, accesses, processes and otherwise uses information on our behalf or in an official capacity – both IT and non-IT users.	- Follow policies, standards, procedures and guidance, and protect council information, devices, information storage facilities and processing systems in line with them. - Keep up to date with: - mandatory training; and - general awareness communications.