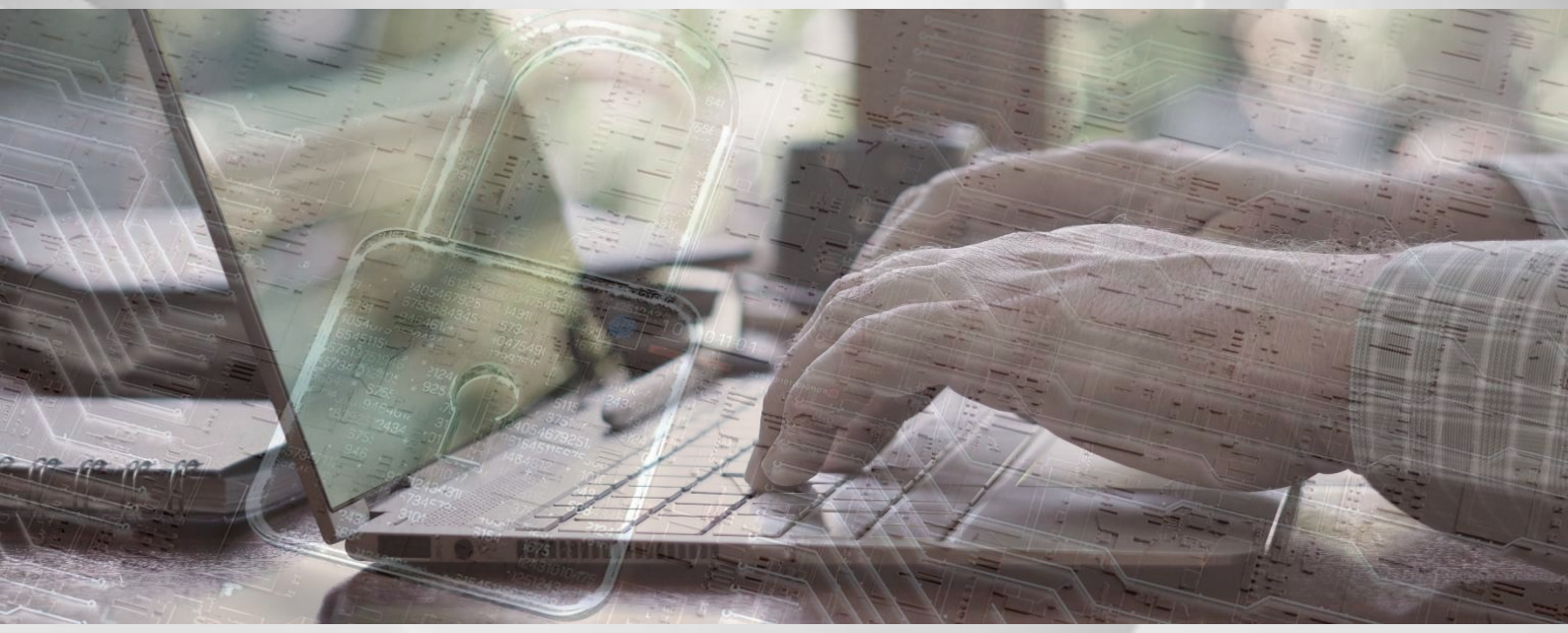
NORTH LANARKSHIRE COUNCIL
COMHAIRLE SIORRACHD LANNRAIG A TUATH

INFORMATION AND CYBER SECURITY POLICY

VERSION 5.01, MARCH 2026



LIVE
LEARN
WORK
INVEST
VISIT

Document control			
Title	**Information and Cyber Security Policy**		
Owner	Chief Officer (Legal, Democratic and Strategy)	**Contact**	InformationRiskAndAssuranceTeam@northlan.gov.uk
Governance group	Data Governance Board		
Author	Information Compliance Officer	**Contact**	InformationRiskAndAssuranceTeam@northlan.gov.uk

Revision history

Number	Originator	Date review commenced	Revision description/record of change
5.0	Information Risk Manager	14 February 2025	Two-yearly review and change of writing style from second to third person.
4.0	Information Risk Manager	03 May 2023	Two-yearly review and plain English changes.
3.0	Information Risk Manager	09 March 2021	Review with aim of deprecating Information Risk and Information Classification and Handling policies.
2.1	Information Risk Manager	18 February 2021	Reviewed as part of review of all information governance policies and guidelines.
2.0	Information Risk Manager	28 April 2020	Regular review including comments from Data Governance Board and Data Management Team.

Document approvals

Number	Governance group	Date approval granted	Date approval to be requested (if document still draft)
5.0	Policy and Strategy Committee	19 March 2026	
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)		
Status of document consulted upon	Stakeholders consulted between 11 March 2025 and 22 December 2025.	
Stakeholders consulted and dates	Data Management Team Technology Strategy Manager Data Governance Board Corporate Management Team	11 March 2025 11 March 2025 26 March 2025 22 December 2025

Strategic alignment

Plan for North Lanarkshire

Improving North Lanarkshire's resource base – Build a workforce for the future capable of delivering on our priorities and shared ambition.

Strategic alignment (continued)

Digital and IT Strategy

The Digital and IT Strategy is critical to enabling the Council to deliver on its vision. It sets the standards and provides the direction for the strategies, policies, and plans which enable the delivery of critical public services, business as usual activities and the investment programmes of work.

The Information and Cyber Security Policy is one of these. It supports the strategy by providing a safe framework for using Council information, and information storage facilities and processing systems without exposing the Council or its users to unacceptable risks.

Next review date

Review date	March 2028

Contents

1 Introduction

Information is a critical asset. North Lanarkshire Council (the Council) relies on physical and information technology (IT) assets to use, store, manage, process, and share information.

This policy sets out how the Council – and anyone who operates on its behalf to deliver or supply services – manages, secures and protects its information. This allows the Council to continue to deliver services, carry out statutory duties, and support internal business functions. It covers the following.

1. **Physical access** to electronic and paper-based information assets including Council and other buildings where it conducts business, or third parties operate on its behalf.
2. **Logical access** to electronic information, and IT systems and services, both hosted within the Council IT network and cloud-based – including laptops and mobile phones, business and communications systems, office software, databases, websites, and apps.
3. **Network infrastructure and services** including hardware and software, both within the Council network and through cloud managed services – including routers, switches, 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 the Council's customers, service users, employees and other authorised IT users.
7. **Managing information and cyber security threats** to information in all formats and all the Council's IT assets, including networks, systems and devices.
8. **Third-party supplier and service provider security**, particularly where third parties hold or process the Council's information on its behalf.

Information security: Measures to protect information in all formats – digital, physical, and spoken – from unauthorised or unintended access, disclosure, use, or destruction.

Cyber security: Measures to protect IT assets and digital information from cyber attacks, which the National Cyber Security Centre (NCSC) defines as:

> **"attempt[s] to damage, disrupt or gain unauthorised access to computer systems, networks or devices."**

As the Council takes a digital by default approach to service delivery and much of its information is now in digital format, this is a critical branch of its information governance approach.

The Council owns all information it stores. It securely manages this along with the devices, systems, and services it uses to create, store, access and process it.

2 Purpose

This policy provides a framework to effectively manage information and cyber security, helping to protect Council information from theft, loss, and unauthorised access or disclosure.

It balances the benefits and risks of processing information, in line with the three core principles of information security – known as the CIA triad.

Confidentiality

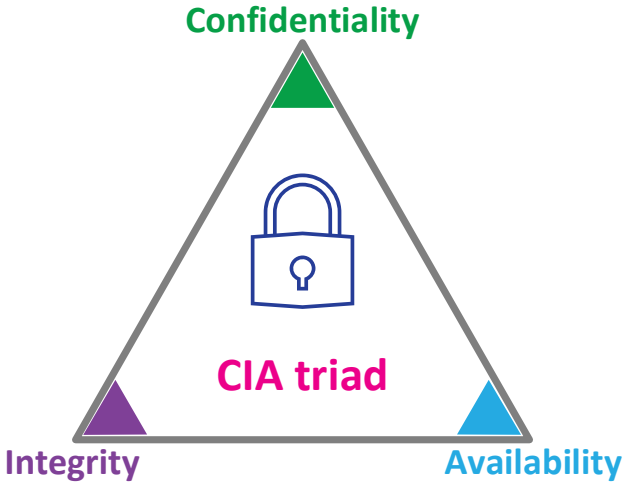
Only those who should see it, do see it.

Integrity

Information is correct and kept up to date, and only used for its intended purpose.

Availability

Authorised users have access to information when they need it.



This policy defines the security measures designed to protect and minimise threats to all three elements of the CIA triad for information at the **OFFICIAL** tier, as per the UK Government's Security Classification Policy. It is a corporate risk control factor and aligns with the following.

- Digital and IT Strategy – this brings together separate but related plans and policies, including this one, that contribute to the Council's digital vision.
- Its sister policies that help secure information.
  - Data Protection
  - Payment Card Data Security
  - Records and Information Management
- Acceptable Use of IT Policy – this informs the Council's IT users on how to appropriately use IT assets to access, store and process information.
- Codes of conduct that set out mandatory standards for Councillors, Chief Officers, and Employees, in particular relating to privacy and confidentiality.
- Any third-party supplier or service provider contractual compliance obligations.
- Legislative and regulatory compliance obligations and guidance. This includes:
  - Computer Misuse Act 1990
  - Copyright, Designs and Patents Act 1988
  - Cyber Resilient Scotland: strategic framework – Public Sector Action Plan

- Data Protection Act 2018
- General Data Protection Regulations
- Government Security Classifications
- Payment Card Industry Data Security Standard
- Public Bodies (Joint Working) (Scotland) Act 2014
- Public Records (Scotland) Act 2011
- Public Services Network Connection Compliance

3 Scope

This policy applies to all aspects of information and cyber security, including the following.

1. All IT assets – systems, services, and devices – that the Council uses to store, process, transmit or receive information – including how it specifies, designs, develops, installs, operates, connects, uses, and decommissions them.
2. All information assets – data, files, documents, records and knowledge – that it creates or receives from third parties, stores and processes in the following formats.
    - **Digital:** IT and communication systems containing data, records, and digital files – such as documents, audio, video, images - hosted within the Council IT network and on cloud-based services; or stored on removable media.
    - **Paper:** Printed or handwritten, stored in Council and authorised third-party locations.
    - **Spoken:** Two or more people communicating by talking or using sign language – in person, over the phone, in online meetings – including using interpreters for signing and spoken languages other than English. One way communication using technology that supports dictation and read aloud functionality.
3. Every authorised person who creates, accesses, processes, and otherwise uses information on the Council's behalf or in an official capacity – both IT and non-IT users. This includes all employees, elected members, contractors, consultants, third-party suppliers and service providers, temporary agency staff, modern apprentices, students, volunteers, and anyone else with authorised access.

4 Governance

The **Policy and Strategy Committee** has **approval** authority for, and oversight of, this policy.

The **Data Management and Compliance Group** (formerly 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 Legal, Democratic and Strategy** – as the Council's Senior Information Risk Owner – is **accountable** for its governance.

The **Information Risk and Assurance 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 instructions and guidance on how to apply and comply with this policy through frameworks, standards, procedures, and guidance – 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, or an audit action.
    b. Report to management teams, governance and working groups, committees, and scrutiny panels.

5 Policy compliance

Every person with access to Council information and who uses it while working on behalf of the Council or in an official capacity, must comply with this policy, and all the policies, standards, procedures, and guidance it references.

This includes:

1. only using Council information for its intended purpose – unless otherwise authorised;
2. maintaining its confidentiality and integrity;
3. keeping it safe; and
4. only using Council managed devices to access Council information and systems, and conduct Council business – subject to limited exceptions detailed in the Acceptable Use of IT Policy and excluding third parties delivering services on its behalf as defined in individual contracts.

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

- Chief Executive
- Data Governance Board
- Senior Information Risk Owner
- Technology Strategy Manager
- Third-party suppliers and service providers
- Corporate Management Team
- Data Management and Compliance Group
- Information Risk Manager
- All Managers
- Everyone in the scope of this policy.

Important note regarding the acceptable use of IT

Everyone must understand that – in line with the Acceptable Use of IT Policy – the Council:

- routinely carries out a range monitoring activities of its IT assets for compliance, security, operational, performance, and maintenance purposes;
- reserves the right to formally investigate individual usage – by exception and under strict controls – to help identify potential prohibited use or misuse, as per the Discipline Policy; and
- will refer any suspected unlawful acts to the appropriate authorities – this includes the police, and professional and regulatory bodies.

6 Policy objectives

This policy sets the Council's strategic position and lays the foundations for effective information and cyber 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. Show key stakeholders – such as elected members, residents, customers and service users – that the Council treats and protects information in line with its value and sensitivity.
3. Help everyone who accesses or processes Council information to understand:
    a. why they must protect its confidentiality, integrity, and availability;
    b. the controls it uses to protect this information; and
    c. their role in this.
4. Make sure third-party suppliers and service providers:
    a. understand – at an organisational and individual level – their responsibilities and contractual obligations in relation to all relevant security measures; and
    b. can demonstrate their compliance with Council policies, standards and procedures.
5. Provide a framework for security plans, standards, procedures, and guidance – to protect its information, systems, devices and processes.
6. Promote compliance with all legislation and regulations governing its information assets.
7. Maximise the benefits of its information whilst identifying and managing associated information and cyber risks.

7 Security controls

7.1 Managing risk

Managing risk is critical to keeping information secure. This process includes –

- Identifying, assessing, and monitoring risks to information, and information processing systems and storage facilities.
- Preventative mitigations and response planning to manage threats to information and IT assets. These threats include human error, public infrastructure damage or failure, cyber attacks, malicious and unwanted email, social engineering, supply chain security threats, and insider threats.

The Council does the following to manage information risks.

1. Uses network controls, specialist systems and privileged utility programs to protect its IT infrastructure.
2. Produces and promotes information management policies.
3. Produces and promotes security standards, as per its Security Standards Framework. Each standard contains specific minimum security measures.
4. Develops and implement security operational procedures and user guidance.
5. Produces mandatory training for employees and delivers awareness sessions, as needed.
6. Routinely raises awareness about information security, both generally and topic specific. This includes issuing alerts and guidance about specific threats, as they occur.
7. Agrees specific information and cyber risk treatment plans – and invokes them when it needs to – in line with the Risk Management Strategy.

7.2 Managing information

This policy – and related Data Protection, Payment Card Data Security, and Records and Information Management **policies – define how the Council manages and uses information.** It has a range of supporting products, relating to specific elements of this. In particular –

1. **Information classification and handling:** The Information Classification and Handling Security Standard helps everyone:
   - understand the different classes of information and what to use them for;
   - decide which classification to use for an information asset, based on the sensitivity and confidentiality of its content; and
   - know how to protectively mark and handle information based on its classification.
2. **Records retention:** The Records Retention Schedule specifies
   - how long to keep information, and
   - whether to dispose of, archive or permanently preserve it.

3. **Information assets:** The Information Asset Register details all 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.

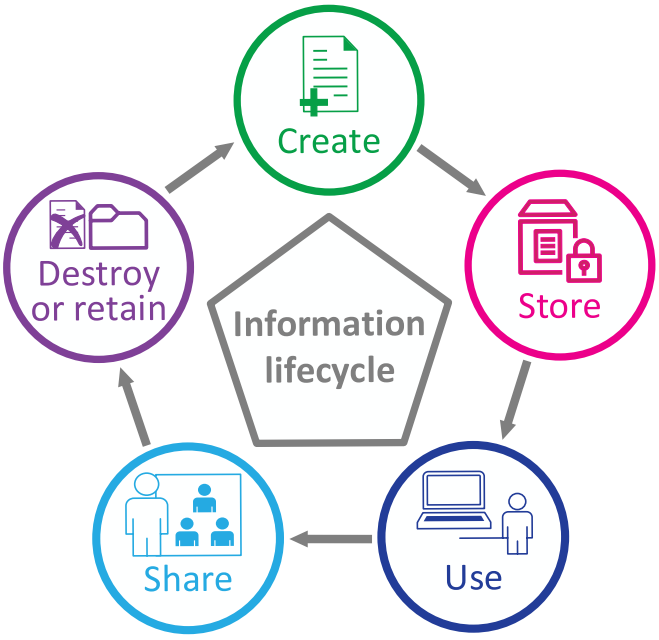
User guidance to help manage information securely

Guidance on the intranet covers specific topics including –

- Email security
- IT authentication (password) and secure access
- Information handling rules
- Remote working security
- SCAM checklist

7.3 Operational security

Information is at the core of all Council operational activities. Procedures and controls securely manage every stage of its lifecycle – covering how to create, store, use, share, and destroy or retain information.



Key operational activities include the following.

1. **Compliance:** Legislation and regulations, data sharing arrangements and contractual obligations.
2. **People resources procedures:** Recruitment, disclosure and other vetting processes.

3. **Access control:** How to control access to information and systems. This comprises the following.
    3.1. **User access** including identity and access management, provisioning, privileged access management, passwords and other authenticators, and user authentication and secure access responsibilities.
    3.2. **Device access** including Council and personal devices.
    3.3. **Access to IT systems and services** including system controls to protect against unauthorised access, service disruption, data breach and data loss.
    3.4. **Access to network infrastructure and services** including network controls and procedures, and privileged utility programs.
    3.5. **Access to electronic information** using permissions, privileges, and cryptography, depending on the information sensitivity.
    3.6. **Third party access** as defined in Code of Connection procedures.
4. **IT operational controls:** This includes products and procedures to manage change, protect and manage the Council IT network infrastructure, introduce, and decommission systems, and replace and dispose of hardware.
5. **Information security incidents:** The Information Security Incident Management Procedure and the Data Protection Breach and Incident Management Protocol explain how to respond to actual and suspected security incidents.
6. **Business continuity:** The Business Continuity Guidance explains the provisions in place as part of the resilience function. This includes a corporate business continuity plan and service level plans, business continuity champions, and testing and review arrangements.
7. **Disaster recovery:** The IT Systems Resiliency and Disaster Recovery Standard classifies IT systems in terms of how critical they are to service delivery and business continuity.
8. **Third-party procurement:** The Corporate Procurement model includes governance arrangements, procedures for engaging with suppliers and service providers, and procurement toolkits and templates. The Purchasing Cloud-Services: Cyber Security Procedure explains the processes to evaluate third-party supplier and service provider security when buying and commissioning cloud-based IT solutions.
9. **Project management controls:** The Project Management Framework includes records management, data protection and information security guidance for its product set

7.4 Cyber security

Technical security measures align to the NIST Cyber Security Framework (CSF). This is a taxonomy of **high-level cyber security outcomes** that help manage cyber security risks. Its core components are a hierarchy of functions, categories, and subcategories that detail each outcome. The Council uses the CSF for the following reasons.

1. It meets the requirements of Enterprise Architecture Business Principle 2 – Reuse before buy, before build.

2. It is an internationally adopted common and open framework.
    a. Its open nature means it's usable without the need for extensive resources, continual certification, or costly audits.
    b. The outcomes are sector, country, and technology-neutral, giving the flexibility to tailor it to suit the Council's specific needs in terms of risks, technologies, and priorities.
    c. It is outcomes-based, focusing on what the Council needs to achieve, not how to do it.
    d. It has a strong emphasis on governance, which aligns with the Council's strategic vision, information governance policies and compliance obligations – as set out in the introduction of this document.
3. It provides reporting advantages.
    a. The security outcomes are easy to understand for a broad audience, regardless of their cyber security expertise.
    b. It's measurable against a range of security frameworks as required.

The CSF comprises the following core functions and each of these contains a series of related categories listed in Appendix B.

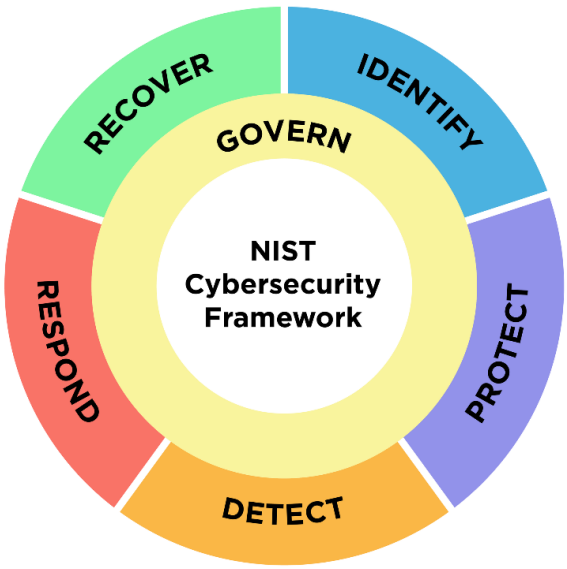
Govern:
Establish, communicate, and monitor cyber security risk management strategy, expectations, and policy.

Identify:
Understand current cyber security risks.

Protect:
Safeguards to manage cyber security risks.

Detect:
Find and analyse possible cyber security attacks and compromises.

Respond:
Actions regarding a detected cyber security incident.



Recover:
Restore assets and operations affected by a cyber security incident.

7.5 Third-party supplier and service provider security

The Digital and IT Strategy sets out a vision for a **Digital North Lanarkshire**, including taking a **cloud first** approach to IT solutions, in the following order of preference.

1. Software as a Service (SaaS)
2. Platform as a Service (PaaS)
3. Infrastructure as a Service (IaaS)

All third parties the Council contracts with to operate on its behalf by providing services and solutions must take a risk-based approach to information and cyber security. They must apply the following.

- Security controls and measures that align with Council security policies, frameworks, plans, standards, and procedures.
- Employee recruitment and human resources policies that are the same or similar to the Council's own.
- All contractually agreed information security obligations and accountability.

7.6 Training and awareness

Training and awareness both help manage information risk. By giving people the knowledge and confidence they need to carry out their information and cyber security responsibilities, this helps change behaviours to further protect information and systems.

A series of **mandatory training courses** on LearnNL cover the core elements of information governance – data protection, information and cyber security, and records and information management. Employees must complete these courses every two years to keep up to date with any changes in policy or legislation.

The Council carries out a range of **awareness raising** activities using different types of media and systems to promote information and cyber security, share information and build knowledge. This is generally aimed at everyone but may also target specific audiences.

Awareness raising

Activities: To 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.
- Conducting regular phishing simulation exercises to train users in detecting and reporting scam messages, to mitigate the risk of a successful phishing attack.
- Issuing alerts and guidance about specific threats, as they occur – for example, a new phishing scam designed to steal information.
- Engaging directly through the Information and Cyber Security Viva Engage community, including answering questions, asking for opinions, and linking to other useful content.
- Notifying users of policy changes, new standards, procedures and guidance.
- Delivering general or topic-specific awareness sessions. These may target particular groups such as elected members, senior managers, or an individual functional area.

Media: Including the following.

- Viva Engage community page
- Intranet document libraries
- Staff announcement emails
- Council news on the intranet
- Email phishing simulator software
- Chief Executive's newsletter
- Popup notifications on Council devices
- PowerPoint presentations

8 Product set

The table below lists products referenced throughout this document. This may include links to other file types, websites and IT systems.

- Those listed under strategies, policies, frameworks, standards, procedures, guidance, and related products are Council products. As per the note at the start of this policy, there are no active hyperlinks to files and web services used exclusively by council staff and elected members.
- Those listed under legislation, regulations, and government guidance are the responsibility of other agencies.

Product type	Product
Strategies	▪ Digital and IT Strategy ▪ Risk Management Strategy
Policies	▪ Acceptable Use of IT Policy ▪ Data Protection Policy ▪ Discipline Policy ▪ Payment Card Data Security Policy ▪ Records and Information Management Policy
Frameworks	▪ Corporate Procurement model ▪ Project Management Framework ▪ Security Standards Framework
Standards	▪ Code of Conduct for Chief Officers ▪ Employee Code of Conduct ▪ IT Systems Resiliency and Disaster Recovery Standard ▪ Information Classification and Handling Security Standard
Procedures	▪ Code of Connection procedures ▪ Data Protection Breach and Incident Management Protocol ▪ Information Security Incident Management Procedure
Guidance	▪ Business continuity guidance ▪ Email security guidance ▪ Intranet document library ▪ IT Authentication (Password) and Secure Access User Guidance ▪ Purchasing Cloud-based Services Cyber Security Guidance ▪ Quick guide to information handling rules ▪ Quick guide to remote working security

Product type	Product
Guidance (continued)	▪ SCAM checklist ▪ Viva Engage community page
Related products	▪ Council news on the intranet ▪ Information Asset Register ▪ LearnNL ▪ Records Retention Schedule
Legislation, regulations, and government guidance	▪ Computer Misuse Act 1990: GOV.UK ▪ Copyright, Designs and Patents Act 1988: GOV.UK ▪ Councillors' Code of Conduct ▪ Cyber Resilient Scotland: strategic framework – Public Sector Action Plan: GOV.SCOT ▪ Cyber Security Framework: NIST ▪ Data Protection Act 2018: GOV.UK ▪ General Data Protection Regulations ▪ Government Security Classifications: GOV.UK ▪ Government Security Classification Policy: GOV.UK ▪ Public Bodies (Joint Working) (Scotland) Act 2014: GOV.UK ▪ Public Records (Scotland) Act 2011: GOV.UK ▪ Payment Card Industry Data Security Standard: PCI ▪ Public Services Network Connection Compliance: GOV.UK

Appendix A: Information and cyber security roles and responsibilities

Role	Responsibilities
Chief Executive of North Lanarkshire Council.	▪ Overall accountability for the protection of information the Council owns and processes.
Senior Information Risk Owner (SIRO) The Chief Officer of Legal, Democratic and Strategy has this role.	▪ Make sure the Council protects both its information, and its information storage facilities and processing systems. ▪ Accountable for information and cyber security governance.
Corporate Management Team Members are the Chief Executive, Depute Chief Executive, SIRO, and Chief Officers.	▪ Sign off on information and cyber security controls and practices. ▪ Consider reports on the effectiveness of information and cyber 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 and Compliance Group
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 group:
	  ▪ oversees the review of this policy; and
	  ▪ agrees revisions before passing to the Data Governance Board to consider.

Information Risk Manager
Lead subject matter expert on information and cyber security risk and assurance management.
	▪ Co-ordinate and monitor activities to manage the Council's information risk posture, including:
	  ▪ network controls, specialist systems, and privileged utility programs to protect the IT infrastructure; and
	  ▪ mandatory training and awareness raising.
	▪ Produce and promote this policy and related standards, procedures and guidance.

Role	Responsibilities

Technology Strategy Manager
Responsible for managing the Council IT infrastructure.
	▪ Implement, manage and monitor technical security measures, in line with appropriate security standards to protect the Council's
	  ▪ IT infrastructure,
	  ▪ IT assets, and
	  ▪ digital information assets managed or stored by Technology and Digital Strategy services.

All managers
Anyone responsible for managing a function or group of people within the Council. This includes information, IT asset and product owners.
	▪ Make sure processes and security controls are in place to manage information effectively.
	▪ Make sure staff members:
	  ▪ understand their compliance responsibilities and the consequences of non-compliance;
	  ▪ follow policies, standards, procedures and guidance; and
	  ▪ keep up to date with mandatory training.

Third-party suppliers and service providers All third-party organisations and their individual employees that the Council contracts to operate on its behalf by providing services and solutions.	▪ Understand their compliance responsibilities and the consequences of non-compliance, as contractually agreed.

Everyone
As per the scope, every person who creates, accesses, processes and otherwise uses information on behalf of the Council 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.

Appendix B: Cyber Security Framework core functions and categories

Extracted from the NIST Cyber Security Framework

Function	Category	NIST ID
Govern	Organisational context	GV.OC
	Risk management strategy	GV.RM
	Roles, responsibilities and authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity supply chain risk management	GV.SC
Identify	Asset management	ID.AM
	Risk assessment	ID.RA
	Improvement	ID.IM
Protect	Identity Management, authentication, and access control	PR.AA
	Awareness and training	PR.AT
	Data security	PR.DS
	Platform security	PR.PS
	Technology infrastructure resilience	PR.IR
Detect	Continuous monitoring	DE.CM
	Adverse event analysis	DE.AE
Respond	Incident management	RS.MA
	Incident analysis	RS.AN
	Incident response reporting and communication	RS.CO
	Incident mitigation	RS.MI
Recover	Incident recovery plan execution	RC.RP
	Incident recovery communication	RC.CO