Information Security Policy

Version 3.0, 26 March 2021

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.

LIVE
LEARN
WORK
INVEST
VISIT

Document Control

Organisation	North Lanarkshire Council
Title	Information Security Policy Version 3.0
Creator	Information Risk Manager
Owner	Senior Information Risk Officer
Subject	The Security Policy formalises Information Security within North Lanarkshire Council
Classification	OFFICIAL
Identifier	20210326 Information Security Policy Version 3.0
Date Issued	4 June 2021

Revision History

Revision	Originator	Date of revision	Revision Description
1.1	Linda Caldwell	22/02/2013	Regular Review
1.2	Linda Caldwell	16/08/2014	Document controls modified in line with
1.3	Linda Caldwell	15/11/2016	Regular Review
2.0	Rob Leitch	28/04/2020	Regular Review including comments
2.1	Charles Muir	18/02/2021	Reviewed as part of review of all Information Governance policies / guidelines
3.0	Rob Leitch	09/03/2021	Further review with aim of deprecating Information Risk Policy and Information Classification & Handling

Document Approvals

Sponsor Approval	Revision No.	Date
Policy and Resources	1.1	14/03/2013
Policy and Resources	1.2	16/09/2014
Policy and Resources	1.3	21.06.2017
Policy and Strategy Committee	2.0	11.06.2020
Policy and Strategy Committee	3.0	03.06.2021

Document distribution and communication

This document will be made available to All Users. It will be published on the corporate intranet. Staff will be informed by periodic staff notices and induction information

Contents

1. Introduction

1.1 Information is critical to North Lanarkshire Council and its employees, customers, partner agencies and other stakeholders. Information systems and physical assets including supporting processes, networks and equipment must be protected to ensure the council can continue to operate.

1.2 For organisations such as the council the aim of information security is to enable the successful delivery of functions, whilst finding the right balance between the benefits and risks to the processing of information. How we handle, process, exchange, and store information are clearly of importance, as are the ICT systems that we have come to rely on. Information security must address a range of concerns including:

- Physical access to electronic and paper-based information assets
- Logical access to data, systems, applications, and databases
- External and internal access to networks and all other computing resources including cloud resources
- Legislation impacting data and IT systems in all council locations, business units and teams
- Compliance requirements and standards set out by Government, partner organisations, and regulatory bodies
- Consumer and employee privacy rights
- Supply chain security, particularly where a third party holds or processes information on the council's behalf

2. Purpose

2.1 This policy sets the strategic position and lays the foundations and framework for effective information security. The key objectives of this policy are to:

- Show clear executive-level understanding of the value of information and the need for making resources available for its protection
- Demonstrate to all council staff the reasons why we must protect the confidentiality, integrity, and availability of council information
- Show to our key stakeholders such as elected members and the wider community that the council will treat and protect information in accordance with its value
- Provide the framework for the creation of standards, procedures, and guidance relevant to information security.
- Promote compliance with all relevant legislation and regulations regarding council information assets.
- Enable the council to maximise the benefits of the information it holds whilst identifying and managing associated information risks.

3. Governance and Information Security

3.1 The council will ensure appropriate resources are put in place to manage the security of its information and the systems that may store and process it.

3.2 All staff and individuals with access to council information have a responsibility to ensure it is treated appropriately. Employees, Elected Members, third parties and other individuals who may access council information and ICT systems on the council's behalf must adhere to this policy.

3.3 Key individuals and groups in terms of supporting and promoting this policy are:

- Chief Executive
- Senior Information Risk Owner
- Corporate Management Team
- All Managers
- Information Risk Manager
- Data Governance Board
- Data Management Team
- All Staff

3.4 The remit of these groups in managing and implementing this policy is described in Appendix A.

3.5 This policy forms part of the council's Information Governance Policy Framework.

4. Risk Management

4.1 Central to information security is the identification, assessment, and monitoring of risks to council information and information processing assets. The council will put in place appropriate guidance and processes, and where necessary treatment plans, to ensure information risks are identified and managed appropriately.

5. Asset Management and Classification

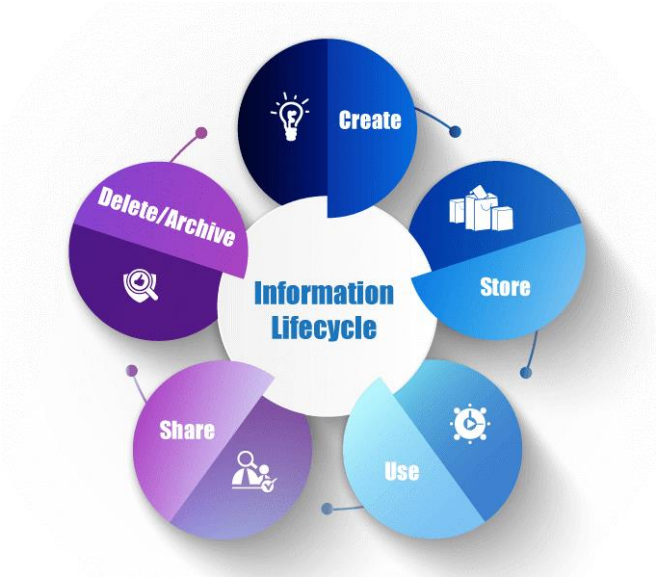
5.1 The council's Information Asset Register provides an inventory of each information asset and identifies the asset owner, classification level (ergo protective marking), location, and with whom it is shared. Published guidance will assist both managers and users in general in judging what classification level should be applied to different types of information and how each level should be handled.

6. Training and Awareness

6.1 A central plank to managing information risk is to ensure anyone creating and using council information is made aware of relevant risks and how these can be addressed. But more than awareness is often required; it is often necessary to change behaviours so that information and information processing systems are protected in practice. The council shall ensure adequate programmes of awareness raising and training take place and that these target relevant audiences.

7. Security in Operational Activities

7.1 Consideration of information security must be part and parcel of all council practices. And in turn security must be considered at all stages of the information lifecycle.



7.2 From an operational perspective, the following activities all have a crucial bearing on securing information assets:

- Human resources activities.
- How we control access to information, primarily through applying ICT controls such as user access management policies, password controls, network access controls, operating system access controls, application access controls, and access to mobile computing and remote working technologies.
- Physical and environmental security to prevent unauthorised access, loss, theft, damage and interference to the council's premises and information assets.
- Operation of day-to-day ICT management activities such as change control, protection against malicious software, general housekeeping duties, network management, handling of media, and decommissioning/disposal of equipment.
- The acquisition, development, and maintenance of ICT systems.
- Information security incident management.
- Business continuity management.
- Compliance with relevant laws, regulations, and contracts (legislation is listed in the Information Governance Policy Framework)

8. Further Information

8.1 For further information about this policy and associated guidelines can be found in the Information Governance Framework area on connect. Should you require additional support or guidance please email nlcitsecurity@northlan.gov.uk.

Appendix A

Role	Description	Responsibilities
Chief Executive	Chief Executive of North Lanarkshire Council	• Overall accountability for the protection of information owned and processed by North Lanarkshire Council.
Senior Information Risk Owner (SIRO)	An individual assigned the role of Senior Information Risk Owner	• Responsible for ensuring council information and information processing assets are appropriately protected and that governance processes exist to manage the key aspects of information security.
Corporate Management Team	The council's executive board comprising the Chief Executive, SIRO, and other executive Heads of Service.	• Receives reports and signs off on the adequacy of information security practices.
All Managers	Anyone with responsibility for managing a function or group of staff within North Lanarkshire Council. This includes information owners.	• Ensuring appropriate processes are in place to manage information effectively, that appropriate information security controls are in place, and that key guidance is adhered to.
Information Risk Manager	The lead subject matter expert on information security and information risk management within North Lanarkshire Council.	• Responsible for putting in place and implementing an action plan of activities to manage the council's information risk posture. • Developing information security policy, standards, and guidance.
Data Governance Board	A cross-council panel comprising Business Data Owners and Subject Matter Experts.	• Chaired by the SIRO, it is assigned responsibility for assuring appropriate implementation of the Information Governance Framework.
Data Management Team	A cross-service panel with business data stewards from all services, chaired by the council's information management subject matter expert.	• Ensuring implementation of information security management policies and guidance within services. • Reviewing and agreeing security policies
All Staff	Anyone accessing NLC information in an official capacity.	• Protecting council information and information processing systems.