

# North Lanarkshire Council Report

## Policy and Strategy Committee

Does this report require to be approved?  Yes  No

Ref REB/FE Date 19/03/26

## Information Governance Policies and Guidance: Two-yearly Review and Update 2025

**From** Rachel Blair, Chief Officer (Legal and Democratic)

**E-mail** BlairR@northlan.gov.uk **Telephone**

### Executive Summary

Consistent with North Lanarkshire Council's Strategic Policy Framework, all information governance policies are embedded as sub-policies within the Digital and IT Strategy 2024–2027, approved by the Policy and Strategy Committee in March 2024.

The following four information governance policies form a critical part of the governance framework that underpins the delivery of the Digital and IT Strategy 2024–2027:

1. Data Protection Policy
2. Payment Card Data Security Policy
3. Information and Cyber Security Policy
4. Records and Information Management Policy

These policies are subject to a formal review cycle every two years to ensure continued compliance with legislative requirements, alignment with recognised good practice, and consistency with the Council's strategic objectives. The previous review of these policies was approved by the Policy and Strategy Committee in June 2023.

The scheduled two-yearly review was completed in 2025. As a result of this review, each policy has been updated to reflect organisational changes, developments in legislation and regulatory expectations, and the Council's evolving digital operating environment. The revised policies are attached to this report for consideration and approval. The next formal review is scheduled for 2027.

Supporting guidance, standards and procedural documentation associated with each policy are maintained on a continuous improvement basis. These materials are reviewed, updated and communicated as required to support effective implementation across the organisation.

### Recommendations

It is recommended that Policy and Resources Committee:

- (1) Approves the updated information governance policies as attached to this report, noting that they have been reviewed in line with the Council's approved review cycle and updated to reflect current legislative requirements, organisational arrangements and recognised good practice; and

- (2) Acknowledges that the next scheduled review of these policies will take place in 2027, or earlier where required to reflect legislative change, regulatory requirements, emerging risks or developments in best practice.

---

## The Plan for North Lanarkshire

Priority	All priorities
Ambition statement	All ambition statements
Programme of Work	Statutory / corporate / service requirement

---

### 1. Background

- 1.1 The vision for a Digital North Lanarkshire is a key priority within the Council's Programme of Work for 2023–2028, as approved by the Policy and Strategy Committee in March 2023. This vision focuses on developing a skilled and digitally capable workforce, fostering an innovative and sustainable organisational culture, and providing strong digital leadership to support the continued social and economic development of North Lanarkshire.
- 1.2 In March 2024, the Policy and Strategy Committee approved the Digital and IT Strategy 2024–2027. This strategy provides the strategic direction required to embed digital thinking into the Council's everyday behaviours, decision-making and service delivery models. It promotes a digital-first approach, ensuring that employees consistently consider how digital solutions can improve efficiency, resilience, security and the customer experience.
- 1.3 The secure management of information and IT assets is fundamental to the effective delivery of Council services and to maintaining public trust. The Data Protection Policy, Payment Card Data Security Policy, Information and Cyber Security Policy, and Records and Information Management Policy are therefore key enabling sub-policies of the Digital and IT Strategy 2024–2027.
- 1.4 Compliance with these policies is mandatory for all individuals who access, use, manage or process Council information in the course of Council business or in an official capacity. This includes Council employees, elected members, contractors, partners and any other individuals granted authorised access to Council information or systems. Compliance is supported by a framework of standards, procedures and guidance.
- 1.5 The Council undertakes regular reviews of its information governance policies to ensure that they remain aligned with current legislation, regulatory requirements and recognised good practice. The previous two-yearly review was approved by the Policy and Strategy Committee in June 2023. The 2025 review has now been completed, and the updated policies are presented at Appendices 1 to 4 of this report.
- 1.6 The next scheduled review of these policies will take place in 2027, unless earlier review is required due to legislative or organisational change.

---

### 2. Report

- 2.1 The Data Protection Policy, Payment Card Data Security Policy, Information and Cyber Security Policy, and Records and Information Management Policy are reviewed on a

two-yearly basis to ensure they remain accurate, effective and aligned with the Council's strategic vision for a Digital North Lanarkshire, as set out in the Digital and IT Strategy 2024–2027.

- 2.2 The last formal review of these policies was approved by the Policy and Strategy Committee in June 2023. The 2025 two-yearly review has now been completed.
- 2.3 The review process was led by the Data Governance Board and the Data Compliance Management Team, with specialist advice and input provided by relevant subject matter experts across the Council. This approach ensured that the revised policies reflect both strategic governance requirements and operational realities.
- 2.4 In addition to the core policy documents, the Council maintains a suite of supporting standards, procedures and guidance to support effective implementation. These supporting documents are reviewed and updated on an ongoing basis to reflect policy changes, emerging risks and evolving best practice.
- 2.5 The updated policies attached as Appendices 1 to 4 have been revised to align with the corporate policy template and plain English requirements. All hyperlinks have been reviewed and updated. A summary of the key changes arising from the 2025 review is provided in sections 2.6 to 2.9 below.

### **Summary of Key Changes to Policies**

#### **Data Protection Policy – Version 8.0 (Appendix 1)**

- 2.6 As part of the 2025 review, the Data Protection Policy has been updated to reflect organisational changes, strengthen governance arrangements, and provide additional clarity on key aspects of data protection compliance. The key changes are:
  - 2.6.1 Across the policy, references have been updated to reflect organisational changes, including:
    - Replacement of references to the Business and Digital Service following recent restructure of Council services;
    - Replacement of the Data Management Team with the Data Management and Compliance Group; and
    - Updates to the Data Protection Officer (DPO) and Senior Information Risk Officer (SIRO) roles to accurately reflect the current allocation of these functions;
  - 2.6.2 A new section (9.1.1) has been added to clarify the Council's approach where joint controller arrangements exist. This section emphasises the need for clearly documented roles and responsibilities, transparency for data subjects, and the provision of appropriate privacy notices that clearly explain joint controller relationships and points of contact;
  - 2.6.3 The policy has been updated to reflect the statutory requirement for data processing agreements and to set out the criteria that such agreements must meet;
  - 2.6.4 References to "Business Managers" have been replaced with "Managers" to clarify that the responsibilities set out apply to all managers across the organisation;

- 2.6.5 Section 16 has been expanded to provide additional clarity on the Council's approach to transferring personal data outwith the UK or the European Economic Area; and
- 2.6.6 The term "Special Category Personal Data" has been added to the glossary of terms to improve clarity and consistency.

### **Payment Card Data Security Policy – Version 2.0 (Appendix 2)**

- 2.7 As part of the 2025 review, the Payment Card Data Security Policy has been substantially updated to strengthen governance, improve clarity, and ensure continued compliance with the Payment Card Industry Data Security Standard (PCI-DSS) and wider information security requirements. The key changes are:
  - 2.7.1 The introduction has been expanded to provide greater clarity on the purpose of the policy and its alignment with the Payment Card Industry Data Security Standard (PCI-DSS), including explicit confirmation that compliance with PCI-DSS is mandatory. The purpose section has been revised to align more closely with the Information and Cyber Security Policy and to clearly reflect the core information security principles of confidentiality, integrity and availability. References to legislative and regulatory compliance obligations have also been expanded;
  - 2.7.2 The scope of the policy has been broadened to explicitly include IT and information assets. Governance references have been updated to reflect organisational changes, including updates to the Senior Information Risk Officer (SIRO) role and the renaming of the Information Security and Risk Team to the Information Risk and Assurance Team;
  - 2.7.3 Additional compliance requirements have been introduced, including a requirement that Council-managed devices are used when accessing Council systems, subject to limited exceptions. A call-out box has also been added to highlight IT monitoring activities, in line with the Acceptable Use of IT Policy;
  - 2.7.4 The policy objectives have been updated to align with the Council's new security standards framework. They have been expanded to place greater emphasis on third-party suppliers and service providers, and on compliance with relevant legislative and regulatory requirements;
  - 2.7.5 The structure of the security controls section has been revised to align with the Information and Cyber Security Policy. New sections have been introduced on risk management and information management, with enhanced focus on official-sensitive information, access control, data protection, physical security, incident management, and third-party security responsibilities; and
  - 2.7.6 The appendices have been updated to reflect revised roles and responsibilities, including those of the Senior Information Risk Officer, the Technology Strategy Manager, and third-party suppliers and service providers.

### **Information and Cyber Security Policy – Version 5.0 (Appendix 3)**

- 2.8 Following the 2025 review, the Information and Cyber Security Policy has been updated to reinforce the Council's strategic approach to cyber security, strengthen governance and compliance arrangements, and ensure alignment with the Digital and IT Strategy 2024–2027 and recognised good practice. The key changes are:

- 2.8.1 The policy has been renamed from *Information Security Policy* to *Information and Cyber Security Policy* to better reflect the critical role of cyber security in supporting the Council's digital-by-default approach to service delivery and wider strategic objectives;
- 2.8.2 The purpose of the policy has been strengthened to clearly reference the core information security principles of confidentiality, integrity and availability, alongside relevant codes of conduct and third-party contractual obligations. References to legislative and regulatory compliance have been expanded. The scope of the policy now explicitly includes both IT and information assets;
- 2.8.3 Governance references have been updated to reflect organisational changes. Policy compliance requirements have been strengthened to explicitly reference the use of Council-managed devices, IT monitoring activities, third-party supplier and service provider responsibilities, and alignment with the Council's security standards framework;
- 2.8.4 The security controls section has been enhanced to include expanded risk management provisions, the introduction of the Security Standards Framework, and updated references to incident management. Clearer alignment has been established with business continuity and disaster recovery arrangements, and a dedicated cyber security framework section has been added. Training and awareness provisions have been strengthened to include phishing simulation exercises; and
- 2.8.5 The appendices have been updated to reflect revised roles and responsibilities and to include the core functions and categories of the Cyber Security Framework.

#### **Records and Information Management Policy – Version 6.0 (Appendix 4)**

- 2.9 As part of the 2025 review, the Records and Information Management Policy has been updated to reinforce the importance of effective record-keeping, ensure continued compliance with statutory requirements, and support the Council's broader information governance framework. The key changes are:
  - 2.9.1 References throughout the policy have been updated to reflect organisational changes, revised system and product names, and the consistent use of terminology relating to records retention and management;
  - 2.9.2 A number of enhancements have been made to strengthen the policy, including greater emphasis on the role of robust record-keeping in evidencing Council decision-making and accountability. The definition of public records, as set out in the Public Records (Scotland) Act 2011, has been clarified. Updates have also been made to improve consistency with the Data Protection Policy and to strengthen guidance on records storage, accessibility, business continuity arrangements and secure disposal; and
  - 2.9.3 The glossary has been revised to improve clarity, remove obsolete terminology, and introduce new definitions where appropriate to support consistent understanding and application of the policy.

## **Conclusion**

- 2.10 The updated information governance policies provide a robust and coherent framework to support the secure, lawful and effective management of the Council's information and digital assets. They reflect current legislative and regulatory requirements, align with the Council's strategic ambition for a Digital North Lanarkshire, and incorporate recognised good practice in information governance, cyber security and records management.
- 2.11 Approval of these policies will ensure the Council continues to manage information-related risks effectively, maintain public trust, and provide a strong foundation for the delivery of resilient, digital-first services.

---

## **3. Measures of success**

- 3.1 Success in relation to the information governance policies will be demonstrated through sustained compliance with statutory and regulatory requirements, supported by regular audits, reviews and evidence of effective implementation.

### **Data Protection Policy**

- 3.2 Key indicators include:

- Appropriate identification and completion of Data Protection Impact Assessments (DPIAs)
- A reduction in the number of personal data breaches;
- Appropriate data sharing and data processing agreements in place; and
- Increased awareness of international data transfer requirements and early engagement with the Information Governance Team.

### **Payment Card Data Security Policy**

- 3.3 Key indicators include:

- Compliance with the Payment Card Industry Data Security Standard (PCI-DSS) across all Council payment systems;
- Timely completion of security assessments for all systems processing cardholder data;
- Implementation of appropriate access controls and encryption measures for cardholder information;
- Effective monitoring, reporting, and management of security incidents relating to cardholder data; and
- Assurance that third-party suppliers and service providers meet contractual security obligations.

### **Information and Cyber Security Policy**

- 3.4 Key indicators include:

- Adoption and embedding of the Council's Security Standards Framework across all IT and information systems;
- Reduction in the number and severity of information security and cyber incidents;

- Completion of cyber security training for staff, including phishing simulation exercises;
- Effective management of business continuity and disaster recovery arrangements;
- Evidence of robust risk assessment and mitigation measures for both Council-managed and third-party systems; and
- Regular reporting on compliance with cyber and information security policies to the Data Governance Board and the Business Management Team.

## **Records and Information Management Policy**

3.5 Key indicators include:

- Consistent storage of records in line with Council functions and file plans;
- Compliance with the Records Retention Schedule; and
- Improved organisational awareness of guidance on naming, storing and disposing of records

---

## **4. Supporting documentation**

- 4.1 Appendix 1 – Data Protection Policy – Version 8.0.
- 4.2 Appendix 2 – Payment Card Data Security Policy – Version 2.0
- 4.3 Appendix 3 – Information and Cyber Security Policy – Version 5.0
- 4.4 Appendix 4 - Records and Information Management Policy – Version 6.0.



**Rachel Blair**  
**Chief Officer (Legal and Democratic)**

---

**5. Impacts**

<p><b>5.1 Public Sector Equality Duty and Fairer Scotland Duty</b> Does the report contain information that has an impact as a result of the Public Sector Equality Duty and/or Fairer Scotland Duty? Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> If Yes, please provide a brief summary of the impact?  If Yes, has an assessment been carried out and published on the council's website? <a href="https://www.northlanarkshire.gov.uk/your-community/equalities/equality-and-fairer-scotland-duty-impact-assessments">https://www.northlanarkshire.gov.uk/your-community/equalities/equality-and-fairer-scotland-duty-impact-assessments</a> Yes <input checked="" type="checkbox"/> No <input type="checkbox"/></p>
<p><b>5.2 Financial impact</b> Does the report contain any financial impacts? Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> If Yes, have all relevant financial impacts been discussed and agreed with Finance? Yes <input type="checkbox"/> No <input type="checkbox"/> If Yes, please provide a brief summary of the impact?</p>
<p><b>5.3 HR policy impact</b> Does the report contain any HR policy or procedure impacts? Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> The report focuses exclusively on information governance, data protection, cyber security, payment card security, and records management policies. While these policies apply to all staff, elected members, and authorised users of Council information and IT systems, they do not introduce or amend any employment terms, HR procedures, or staff management policies. Any implications for staff relate solely to compliance with the information governance framework, training, and awareness obligations, rather than formal HR policy changes. If Yes, have all relevant HR impacts been discussed and agreed with People Resources? Yes <input type="checkbox"/> No <input type="checkbox"/> If Yes, please provide a brief summary of the impact?</p>
<p><b>5.4 Legal impact</b> Does the report contain any legal impacts (such as general legal matters, statutory considerations (including employment law considerations), or new legislation)? Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> If Yes, have all relevant legal impacts been discussed and agreed with Legal and Democratic? Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> If Yes, please provide a brief summary of the impact?  The updated information governance policies have been revised to ensure compliance with relevant statutory and regulatory requirements, including data protection legislation (e.g., the UK General Data Protection Regulation and Data Protection Act 2018), the Public Records (Scotland) Act 2011, Payment Card Industry Data Security Standard (PCI-DSS) obligations, and other applicable information and cyber security legislation.  The legal impacts are primarily related to:</p>

- Ensuring the Council meets its statutory obligations for processing, storing, and sharing personal and sensitive information;
- Clarifying responsibilities for compliance with international data transfer requirements;
- Strengthening contractual and legal obligations for third-party suppliers and service providers;
- Supporting legal accountability and evidencing decisions through robust records management practices.

**5.5 Data protection impact**

Does the report / project / practice contain or involve the processing of personal data?

Yes  No

If Yes, is the processing of this personal data likely to result in a high risk to the data subject?

Yes  No

If Yes, has a Data Protection Impact Assessment (DPIA) been carried out and e-mailed to [dataprotection@northlan.gov.uk](mailto:dataprotection@northlan.gov.uk)

Yes  No

**5.6 Technology / Digital impact**

Does the report contain information that has an impact on either technology, digital transformation, service redesign / business change processes, data management, or connectivity / broadband / Wi-Fi?

Yes  No

If Yes, please provide a brief summary of the impact?

Where the impact identifies a requirement for significant technology change, has an assessment been carried out (or is scheduled to be carried out) by the Enterprise Architecture Governance Group (EAGG)?

Yes  No

**5.7 Environmental / Carbon impact**

Does the report / project / practice contain information that has an impact on any environmental or carbon matters?

Yes  No

If Yes, please provide a brief summary of the impact?

**5.8 Communications impact**

Does the report contain any information that has an impact on the council's communications activities?

Yes  No

If Yes, please provide a brief summary of the impact?

The report and the updated information governance policies have implications for the Council's communications activities insofar as they guide the secure and compliant handling of information both internally and externally. This includes:

- Ensuring any communication of personal or sensitive data complies with data protection legislation;
- Requiring that information shared via Council communications channels (e.g., websites, social media, press releases) is managed in line with the Records and Information Management Policy and the Information and Cyber Security Policy;

- Supporting consistent messaging regarding the Council's approach to information governance, cyber security, and data protection obligations when interacting with the public, stakeholders, or partners.

No proactive public communications campaign is required solely as a result of this report; however, staff awareness and internal communications may be required to support implementation of the updated policies.

**5.9 Risk impact**

Is there a risk impact?

Yes  No

If Yes, please provide a brief summary of the key risks and potential impacts, highlighting where the risk(s) are assessed and recorded (e.g. Corporate or Service or Project Risk Registers), and how they are managed?

The report addresses key operational and strategic risks associated with information governance, data protection, cyber security, payment card security, and records management. Risk impacts are highlighted and managed as follows:

- Assessment and Recording:
  - Information-related risks are recorded in the Council's Corporate and Service Risk Registers, including risks relating to personal data breaches, cyber security incidents, and non-compliance with statutory or regulatory obligations.
  - Policy compliance and implementation risks are reviewed by the Data Governance Board and the Data Compliance Management Team.
- Management and Mitigation:
  - Updated policies include clear roles and responsibilities, governance frameworks, and operational controls to mitigate identified risks.
  - Supporting standards, procedures, training, and monitoring mechanisms (e.g., IT system monitoring, phishing simulations, audits) ensure proactive risk management.
  - Third-party risks are addressed through contractual obligations, due diligence, and monitoring of supplier and service provider compliance.

These measures ensure that information governance and associated risks are actively managed in alignment with corporate risk management processes.

**5.10 Armed Forces Covenant Duty**

Does the report require to take due regard of the Armed Forces Covenant Duty (i.e. does it relate to healthcare, housing, or education services for in-Service or ex-Service personnel, or their families, or widow(er)s)?

Yes  No

If Yes, please provide a brief summary of the provision which has been made to ensure there has been appropriate consideration of the particular needs of the Armed Forces community to make sure that they do not face disadvantage compared to other citizens in the provision of public services.

**5.11 Children's rights and wellbeing impact**

Does the report contain any information regarding any council activity, service delivery, policy, or plan that has an impact on children and young people up to the age of 18, or on a specific group of these?

Yes  No

If Yes, please provide a brief summary of the impact and the provision that has been made to ensure there has been appropriate consideration of the relevant Articles from the United Nations Convention on the Rights of the Child (UNCRC).

If Yes, has a Children's Rights and Wellbeing Impact Assessment (CRWIA) been carried out?

Yes  No

# Data Protection Policy

Version 8.0, 19 March 2026

# Document control

<b>Title</b>	Data Protection Policy		
<b>Governance group</b>	Data Governance Board		
<b>Owner</b>	Rachel Blair, Chief Officer (Legal and Democratic)	<b>Contact</b>	<a href="mailto:BlairR@northlan.gov.uk">BlairR@northlan.gov.uk</a>
<b>Author</b>	Colette Cameron, Principal Solicitor (Information Governance)	<b>Contact</b>	<a href="mailto:CameronCol@northlan.gov.uk">CameronCol@northlan.gov.uk</a>

## Revision history

Version	Originator	Review start date	Revision description and record of change
8.0	Colette Cameron	28 July 2025	Bi-annual review.
7.0	Collette Crainie	16 February 2023	Bi-annual review.
6.0	Paul Corrigan	26 March 2021	Bi-annual review.
5.0	Paul Corrigan	30 April 2020	Bi-annual review incorporating feedback from Data Governance Board and Data Management Team.
4.0	Gerry Gardiner	10 May 2018	To reflect the UK General Data Protection Regulations and Data Protection Act 2018.
3.0	Gerry Gardiner	15 November 2016	Bi-annual review.
2.0	Gerry Gardiner	04 July 2014	Data Governance Board consultation.
1.0	Gerry Gardiner	22 February 2013	Data Governance Board consultation.

## Document approvals

Version	Governance group	Date approved	Date approval to be requested (if document still in draft)
8.0	Policy and Strategy Committee		19 March 2026
7.0	Policy and Strategy Committee	08 June 2023	
6.0	Policy and Strategy Committee	03 June 2021	
5.0	Policy and Strategy Committee	11 June 2020	
4.0	Policy and Resources Committee	07 June 2019	
3.0	Policy and Resources Committee	21 June 2017	
2.0	Policy and Resources (Finance and Customer Services) Sub Committee	16 September 2014	
1.0	Policy and Resources (Finance and Customer Services) Sub Committee	14 March 2013	

## Consultation record (for most recent update)

<b>Consultation status</b>	Stakeholders consulted between 15 March 2023 and September 2025	
<b>Stakeholders consulted and dates</b>	Data Governance Board Employment and Policy Team Data Management and Compliance Group Trade Unions (UNISON, UNITE, GMB and EIS)	10 September 2025 27 August 2025 17 February 2026 9 January 2026

<b>Strategic alignment</b>	
<b>Plan for North Lanarkshire</b> 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.	
<b>Digital and IT Strategy</b> The Digital and IT Strategy bring together separate but related plans and policies that contribute to the development and delivery of our digital vision. The Data Protection Policy is one of these. It supports the strategy setting out how we protect personal data using principles, rules, and guidelines to make sure we continue to comply with data protection laws.	
<b>Next review date</b>	
<b>Review date</b>	01 May 2027 or earlier where there are changes to legislation, statutory guidance, or established best practice that require amendment.

# Contents

1. Introduction .....	5
2. Purpose .....	5
3. Scope.....	5
4. Governance.....	6
5. Information risk.....	6
6. Data protection .....	7
7. Personal data.....	7
8. The data protection principles .....	8
9. Discharging our responsibilities .....	9
9.1. The Controller.....	9
9.2. The Data Protection Officer (DPO) .....	16
9.3. The Chief Executive and Chief Officers.....	16
9.4. Business managers.....	17
9.5. All users .....	17
10. Privacy by design and Data Privacy Impact Assessments (DPIAs).....	17
11. Data protection incidents and breaches .....	18
12. Data protection fee.....	19
13. Documenting data processing activities.....	19
14. Sharing information with other Council services and third parties .....	19
15. Data sharing.....	20
16. Transferring personal information outwith the UK or EEA .....	21
17. Rights of individuals.....	21
18. Product set.....	23
Appendix 1: Glossary of terms .....	24

# 1. Introduction

To deliver services effectively North Lanarkshire Council (the Council) needs to collect, process and hold large volumes of information which includes personal information (personal data) relating to current, past and prospective customers, clients, employees, workers, elected members, suppliers, and contractors.

In addition, it may from time to time be required by law to process personal information to comply with the requirements of government departments and other public agencies. There are also instances where we process personal data for contractors and arms' length external organisations and third parties process Council information which includes personal data.

---

**To deliver services effectively we need to collect, process, and hold large volumes of information relating to organisations and individuals. This includes personal data.**

---

## 2. Purpose

This Data Protection Policy sets out how we protect personal data to comply with data protection laws using:

- principles,
- rules, and
- guidelines.

## 3. Scope

This policy is applicable to all personal data held by the Council whether in manual format via Council information technology systems accessed either on Council premises or via mobile or home-working equipment. Personal data held on removable devices and other portable media is also covered by this policy.

The policy applies to all employees, workers, elected members, clients, suppliers, third party contractors and any other individuals or organisations who access Council information.

This policy is not part of the contract of employment, and the Council may amend it at any time. However, it is a condition of employment that employees and others who obtain, handle, process, transport, store, and otherwise process personal data will adhere to the rules of the policy. Any breach of the policy by an employee will be taken seriously and may result in [disciplinary action](#).

Elected members are required, in respect of their use of data, to comply with their obligations as set out in paragraphs 3.21 to 3.23, and 6.2 of the [Councillors' Code of Conduct](#) and paragraphs 70 to 82 of the associated Guidance. Members need to be aware of the potential for personal liability under the relevant legislation, in respect of both criminal and civil court proceedings as well as the imposition of fines by the Information Commissioner.

[Guidance to organisations on the UK GDPR](#) is available from the Information Commissioner's Office website.

## 4. Governance

This policy forms part of a suite of documents that are covered by the [Digital and IT Strategy](#).

The **Data Governance Board** has **approval** authority for, and oversight of, this policy. The **Data Management and Compliance Group** – as **key stakeholders** – oversee its review and consider its contents before referring it on for approval. The **Chief Officer of Legal and Democratic** – as the Council's Senior Information Risk Owner – is **accountable** for its governance. The **Data Protection team** is **responsible** for the following activities:

1. Produce, publish, and promote this policy;
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 every two years, with other reviews when needed. For example, following a critical security incident, new legislation, a significant threat, an audit action; and
4. Report to management teams, governance and working groups, committees, and scrutiny panels.

## 5. Information risk

The collation and holding of information of any nature creates a risk of information falling into the hands of third parties or misuse of the information. To manage those risks the Council has in place a number of policies.

Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times. The Council is exposed to potential fines of up to 20 million Euros (approximately £18 million) or 4% of its total annual turnover, whichever is higher and depending on the breach, for failure to comply with data protection law.

The **Senior Information Risk Owner (SIRO)** is the Chief Officer (Legal and Democratic). The SIRO's duty is in respect of all information collected, held, and processed by the Council. The SIRO is not a position prescribed or regulated by legislation. It is a position recommended by the Information Commissioner. The SIRO is responsible for:

1. overall information risk and they will provide written advice on a regular basis to the Chief Executive on internal control and performance in respect of information risk;
2. assessing the impact of information risks on the Council and how the risks may be managed ensuring arrangements are put in place to mitigate risks. They will implement and lead information risk and management processes within the Council; and
3. advising the Corporate Management Team on effectiveness of information risk management across the Council.

## 6. Data protection

The [UK General Data Protection Regulation](#) (the UK GDPR) sitting alongside the [Data Protection Act 2018](#) (the Act) make provision for how personal data (information) about living individuals in any form including paper and electronic must be collected, processed and held. They impose restrictions on how the Council may process personal data, and a breach of the data protection laws could give rise to criminal and civil sanctions, including fines, as well as adverse publicity.

The legislation also provides that:

1. **special categories of personal data** (that is, data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data, data concerning health, sex life, or sexual orientation); and
2. **personal data relating to criminal offences and convictions** shall only be collected and/or processed for certain specific lawful purposes.

The Council can only process special categories of data and personal data relating to criminal offences and convictions where certain additional conditions apply. The Council has produced an appropriate policy document for such processing.

- For details of conditions for processing special categories of personal data see [Article 9 of the UK GDPR](#) and [Schedule 1 of the Act](#).
- For details of conditions for processing personal data relating to criminal offences and convictions see [Article 10 of the UK GDPR](#) and [Schedule 1 of the Act](#).

## 7. Personal data

This policy adopts the definition of personal data contained in the UK GDPR.

- Personal data is any information relating to an identified or identifiable natural person who can be directly or indirectly identified in particular by reference to an identifier.
- Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

- Personal data that has been de-identified, encrypted or pseudonymised but can be used to re-identify a person remains personal data.
- Personal data that has been rendered anonymous in such a way that the individual is not or no longer identifiable is no longer considered personal data. For data to be truly anonymised, the anonymisation must be irreversible.
- Examples of personal data include:
  - a name and surname;
  - a home address;
  - an email address such as name.surname@company.com;
  - an identification card number;
  - CCTV images of an individual;
  - location data (for example the location data function on a mobile phone);
  - an Internet Protocol (IP) address; or
  - or a cookie ID.
- The following are examples of data which are not considered to be personal data:
  - a company registration number;
  - an email address such as info@company.com; and
  - anonymised data.

## 8. The data protection principles

The UK GDPR requires organisations which handle personal data to collect, process, and hold personal and confidential information securely and responsibly. This includes destroying information safely when it is no longer required.

The UK GDPR sets out the following key principles.

GDPR principle	Description
<b>First: Lawfulness, fairness, and transparency (Section 35 of the Data Protection Act 2018; UK GDPR Article 5(1)(a))</b>	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
<b>Second: Purpose limitation (Section 36 of the Data Protection Act 2018; UK GDPR Article 5(1)(b))</b>	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.

GDPR principle	Description
<b>Third: Data minimisation (Section 37 of the Data Protection Act 2018; UK GDPR Article 5(1)(c))</b>	Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
<b>Fourth: Accuracy (Section 38 of the Data Protection Act 2018; UK GDPR Article 5(1)(d))</b>	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 are erased or rectified without delay.
<b>Fifth: Storage limitation (Section 39 of the Data Protection Act 2018; UK GDPR Article 5(1)(e))</b>	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.
<b>Sixth: Integrity and confidentiality (Section 40 of the Data Protection Act; UK GDPR Article 5(1)(f))</b>	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against: <ul style="list-style-type: none"> <li>▪ unauthorised or unlawful processing, and</li> <li>▪ against accidental loss, destruction, or damage</li> </ul> using appropriate technical or organisational measures.
<b>Seventh: Accountability (UK GDPR Article 5(2))</b>	The Council is also responsible for, and must be able to demonstrate compliance with, the principles.

## 9. Discharging our responsibilities

### 9.1. The Controller

In terms of the legislation, the Council will normally be the Data Controller. In some cases, the Council may be acting as:

- a Joint Data Controller in conjunction with another organisation; or
- a data processor, for example, where it is providing services to an external or arms-length organisation and is processing information of which that organisation is data controller and under their instruction in connection with provision of that service.

To ensure compliance with the data protection principles, the Council will:

- Observe fully conditions regarding the lawful, fair, and transparent collection and use of data.
- Meet its obligations to specify the purposes for which data is used.
- Collect and process appropriate data and only to the extent that it is required to fulfil operational needs or to comply with any legal requirements.
- Ensure the accuracy of the data used.

- Put in place arrangements to determine the length of time the data is held.
- Take appropriate measures to keep the data secure.

### 9.1.1 **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.

## Compliance with the data protection principles

### 1. Lawful, fair, and transparent obtaining and processing

The Council may only collect, process, and share personal data fairly and lawfully and for specified purposes. The law restricts our actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing, but ensure that we process personal data fairly, lawfully and without adversely affecting the data subject.

#### Lawful basis

- It is essential that the legal ground (lawful basis) being relied on for each processing activity is identified and documented.
- The lawful bases for processing personal information are as follows. At least one of these must apply when you process personal data:
  - **Consent** – the individual has given clear consent for you to process their data for a specific purpose.
  - **Contract** – the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
  - **Legal obligation** – the processing is necessary for you to comply with the law (not including contractual obligation).
  - **Vital interests** – the processing is necessary to protect someone's life.
  - **Public task** – the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
  - **Legitimate interests** – the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks).
- **For the majority of processing or personal data carried out by the Council the public task condition will be the appropriate lawful basis**, however, it is very important that the appropriate lawful basis or bases are identified at the outset of the processing activity and these will vary depending on the nature and circumstances of the processing in question.

#### Special category data

- For the processing of special category data, a further additional lawful basis for processing requires to be satisfied. Special category data under data protection law relates to information about an individual's:-
  - race or ethnic origin,
  - politics,
  - religion,
  - trade union membership,
  - genetics,
  - biometrics (for ID purposes),
  - health,
  - sex life, or
  - sexual orientation.

## Compliance with the data protection principles

- There are extensive [lawful bases](#) within [Schedule 1 of the Act](#) for processing in relation to special categories of personal data and data relating to criminal convictions. Advice should be sought from the Information Governance Team via the Data Protection mailbox at [DataProtection@northlan.gov.uk](mailto:DataProtection@northlan.gov.uk) in relation to proposed processing of such data.

### Using personal data

- The Council will be clear when **telling people how their personal information will be used**. This requirement to tell people will always apply, no matter how the information is gathered (for example, paper forms, email, surface mail correspondence, web data collection forms, or any other method). We must say clearly in all of these methods how we will process people's personal information.
- This should principally be achieved by the use of **privacy notices**.
- Privacy notices are a legal requirement. They inform data subjects about the collection and use of their personal data. This relates to the requirement under the legislation that processing of personal data should be transparent.
- Privacy notices should provide individuals with information about our purposes for processing their personal data, how long their data may be retained and with whom it may be shared. This information should be available to individuals at the point of collection of their data. The Council's general [privacy notice](#) and other service specific privacy notices can be found on our website.
- Services should develop their own privacy notices to provide more specific information in relation to particular categories of processing of personal data in relation to their functions. Privacy notices should be regularly reviewed and developed to ensure that they provide accurate and adequate information about the Council's processing activity.

### Consent

In many cases, the Council may process personal information without the **consent** of the data subject where this is required or permitted by law. However, the Council will ask for an individual's **informed consent** if this is needed (the individual must understand what their information will be used for and how it will be shared and stored) ([see first data protection principle](#)). Unless the Council can rely on another legal basis of processing, explicit consent will be required for processing special categories of personal data.

- An individual consents to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. The individual may be asked to sign or to tick a box to give their consent. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.
- Individuals must be easily able to withdraw consent to processing at any time and withdrawal must be promptly acted upon. Consent will need to be refreshed if the Council intends to process personal data for a different and incompatible purpose which was not disclosed when the individual first consented.
- The Council will need to evidence consent captured and keep records of all consents so that we can demonstrate compliance with consent requirements.

## Compliance with the data protection principles

### 2. Purpose limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

- The Council cannot use personal data for new, different, or incompatible purposes from those disclosed when it was first obtained, unless consent is obtained or there is a clear obligation or function set out in law.
- Where information is used for a purpose other than for which it was obtained, privacy information should be updated accordingly to ensure data subjects are so aware.

### 3. Data minimisation

Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. The Council:

- may only process personal data when required to do so in performance of its duties;
- cannot process personal data for any unrelated purposes;
- will not collect excessive data; and
- will ensure that any personal data collected is adequate and relevant for the intended purposes.

When personal data is no longer needed for specified purposes, it should be deleted or anonymised in accordance with the Council's data retention guidelines.

### 4. Accuracy

The Council must make sure that all personal information that it holds is accurate and, where necessary up to date ([see fourth data protection principle](#)).

- Information should be reviewed regularly, and service managers must have procedures in place to make sure that inaccurate or out of date information is updated.
- Information which the Council no longer needs to hold must be destroyed in line with the Council's guidelines on Information Security.

### 5. Storage limitation

Personal data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

- The Council must not keep personal data in a form which permits the identification of individuals for longer than needed for the legitimate business purpose or purposes for which we originally collected it, including for the purpose of satisfying any legal, accounting or reporting requirements.
- The Council will maintain retention policies and procedures to ensure personal data is deleted after a reasonable time for the purposes for which it was being held; unless a law requires such data to be kept for a minimum time.

## Compliance with the data protection principles

- The Council will take all reasonable steps to destroy or erase from our systems all personal data that we no longer require in accordance with all the Council's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.
- Individuals will be informed of the period for which data is stored and how that period is determined.

### 6. Security, integrity, and confidentiality

Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction, or damage.

We will continue to develop, implement, and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of personal data that we own or maintain on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data.

Personal data may only be transferred to third party service providers who agree to comply with the policies and procedures required by the Council and who agree to put adequate measures in place, as requested.

The confidentiality, integrity and availability of personal data must be maintained, that is –

- **Confidentiality:** only people who have a need to know and are authorised to use the personal data can access it.
- **Integrity:** personal data is accurate and suitable for the purpose for which it is processed.
- **Availability:** authorised users are able to access personal data when they need it for authorised purposes.

### 7. Data processors

The law requires the Council to put in place a written contract with each third-party data processor, which contract must meet specific minimum requirements, including procedures and policies to maintain the security of all personal data from the point of collection to the point of destruction. Processing of personal data on the Council's behalf may only take place under the written instruction of the Council and must comply with Section 59 of the Data Protection Act 2018 and Article 28 of the UK GDPR.

Personal data may only be transferred to a third-party data processor if the processor agrees in writing to comply with those minimum requirements.

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's behalf;

## Compliance with the data protection principles

- 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.

### 8. ICO assessments, audits, investigations, and action

The Council must co-operate with any data protection assessment, audit or investigation carried out or action taken by the Office of the Information Commissioner (ICO). Everyone subject to this policy must assist with any such assessment, audit, investigation, or action as required by the ICO and / or the Council.

## 9.2. The Data Protection Officer (DPO)

The Council is required to appoint a DPO. The DPO is currently the Legal Manager (Governance and Information). Their responsibility is in respect of personal data, collected, held, and processed by the Council. They will be involved, properly and in a timely manner, in all issues which relate to the protection of personal data. The DPO's responsibilities include the following:

- Ensuring that
  - the Council complies with the data protection laws,
  - the Council and Council staff are fully informed of their own legal responsibilities and training of staff, and
  - necessary arrangements are in place for dealing where appropriate with [subject access requests](#) that relate to more than one service of the Council.
- Developing and managing the Council's Data Protection Policy, including development, implementation and enforcement of this policy and data protection procedures.
- Reporting on the Council's compliance with the data protection laws to the SIRO on a six-monthly basis.
- Providing advice when requested as regards data protection impact assessments and monitor their performance;
- Co-operating with, acting as a point of contact for, and consulting with the ICO, as required.

## 9.3. The Chief Executive and Chief Officers

The Chief Executive and each Chief Officer's responsibilities include the following.

- Ensuring that
  - the information under their control is collected, processed, and held in accordance with this policy and the data protection laws,
  - necessary arrangements, including nominated officers, are in place to deal with [subject access requests](#),
  - necessary arrangements are in place within their Service for the secure disposal of personal data, and
  - all processing of personal information complies fully with all the provisions of the data protection laws and this policy.
- Nominating lead contacts for data protection responsibility within their Services to the DPO; and immediately reporting changes of contact details to the DPO.
- Identifying and documenting
  - all categories of personal information held within their service,
  - all processing applied to that personal information, and
  - how long personal information needs to be held within each Service.
- Implementing
  - procedures for the secure destruction of any personal information immediately when the Council no longer needs to keep it,
  - arrangements and procedures as necessary for the safekeeping and preservation of all personal information held by their Services and ensuring that no one can get unlawful access to personal information that is held, and

- procedures and issuing instructions to make sure that every person who has access to personal information held by their Service makes use of that information only for the purposes for which that information is held.

## 9.4. Managers

Managers' responsibilities include:

- Ensuring that
  - employees and workers know what they have to do under the data protection laws and are trained in data protection,
  - confirming to the DPO when appropriate training has been undertaken by employees and maintaining records of training,
  - disciplinary action up to the point of dismissal is taken where an employee or worker has deliberately breached the terms of the data protection laws or this policy or of any of the Council's own procedures,
  - employees and workers know that they could face criminal proceedings if they deliberately or recklessly destroy information, obtain information or disclose it unlawfully.
  - personal information held is accurate and up to date.
- Determining whether a [Data Privacy Impact Assessment](#) (DPIA) needs to be undertaken and, if so, putting in place appropriate arrangements to ensure that such a DPIA is undertaken and completed. The DPIA and Guidance can be found at the following link:-  
[DPIA Guidance and Lawful Bases Ver 0.3.docx](#)

## 9.5. All users

All users must:

- Observe and comply with the data protection principles.
- Ensure that:
  - personal information is properly protected at all times – this requires continued compliance with the data protection laws, this policy and all other Council information policies, procedures, and guidance, and
  - individual archives, or any personal records they hold, are not retained when they are no longer required.
- Report any observed or suspected breach of this data protection policy or [related information procedures and guidance](#).

# 10. Privacy by design and Data Privacy Impact Assessments (DPIAs)

We are required to implement **privacy by design** measures when processing personal data by implementing appropriate technical and organisational measures (like pseudonymisation) in an effective manner, to ensure compliance with data privacy principles. Pseudonymisation describes removing or replacing information within data set which identifies an individual.

Users must assess what privacy by design measures can be implemented on all programs, systems and processes that process personal data by considering the following:

- the state of the art;
- the cost of implementation;
- the nature, scope, context, and purposes of processing; and
- the risks of varying likelihood and severity for rights and freedoms of data subjects posed by the processing.

The Council must also conduct DPIAs in respect to high-risk processing.

Services should conduct a DPIA (and discuss the findings with the DPO) when implementing major system or business change programs involving the processing of personal data including:

- use of modern technologies (programs, systems, or processes), or changing technologies (programs, systems, or processes);
- automated processing including profiling and automated decision making;
- large scale processing of special categories of data; and
- large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

1. a description of the processing, its purposes and the Council's legitimate interests, if appropriate;
2. an assessment of the necessity and proportionality of the processing in relation to its purpose;
3. an assessment of the risk to individuals; and
4. the risk mitigation measures in place and demonstration of compliance.

The DPO is responsible for producing guidance on DPIAs and reviewing the guidance every alternate year commencing October 2012.

## 11. Data protection incidents and breaches

The UK GDPR requires data controllers to keep a written record of data breaches, near misses or incidents. This is kept by the Council's DPO.

- Where any breach is assessed as resulting in a risk to the rights and freedoms of the individual(s) affected there is a requirement to notify the ICO of the breach within 72 hours of the breach occurring.
- Where the breach is likely to result in a high risk to the rights and freedoms of affected individuals the UK GDPR requires that the individual(s) is/are informed without undue delay.

All incidents must be reported using the [Data Breach Notification Form](#), whether or not the incident results in a breach of the data protection laws and/or actual damage or loss to any person, to the DPO in accordance with the [Data Protection Breach and Incident Management Protocol](#). To assist you in completing the Data Breach Notification form, please access the relevant guidance [2024\\_06\\_13 Personal Data Breach Guidance.docx](#) The DPO will take appropriate action in respect of the incident, in accordance with the said protocol. Incidents are defined/explained the protocol.

## 12. Data protection fee

It is the responsibility of the DPO to ensure payment of the annual data protection fee to the ICO and to provide all information required by the ICO when doing so.

## 13. Documenting data processing activities

The Council must document and maintain a written record of its data processing activities.

The DPO is responsible for ensuring that all categories of personal information and data subjects held by the Council are documented, including:

1. the uses to which the information is put;
2. the categories of recipients of the personal information;
3. details of transfers to third countries (including the transfer mechanism safeguards in place);
4. the period for which the information will be held; and
5. a description of the technical and organisational measures in place to keep the information secure.

To enable the documentation to be kept up to date at all times, it is the responsibility of the Chief Executive, the Depute Chief Executive and each Chief Officer to advise the DPO immediately of any:

- new categories of information or data subjects held in his/her service;
- changes in the uses to which his/her service is putting any personal information his/her service holds;
- categories of personal information or data subjects which are no longer held by his/her service;
- changes in categories of recipients of personal information held in his/her service;
- changes in the transfer of personal information to third countries (including the transfer mechanism safeguards) in his/her service;
- changes in the retention periods for personal information held in his/her service; and
- changes in the technical and organisational measures in place to keep information secure in his/her service.

## 14. Sharing information with other Council services and third parties

The Council must protect against processing personal information unlawfully. In most cases personal information can only be shared between Council services and/or third parties where the individual concerned knows that such sharing may happen and where the processing complies with the data protection principles. The first data protection principle states that personal information shall be processed fairly, lawfully and in a transparent manner.

Personal data that is provided to a service within the Council is not automatically available to all **other Council services**.

- It is important to understand the purpose or purposes for which the information was originally obtained and whether the data subject would reasonably anticipate that this information would be shared with another Council service.
- Personal information can be shared between Council services where there is a lawful basis to do so, and data subjects are aware of how the data will be used.

Where a request for personal information is received from a **third party**, the identity of the requester and the need for the information must be known before consideration is given to providing it.

- Personal information can be given to the police or the procurator fiscal to help with a criminal investigation and to certain statutory authorities/agencies (such as DWP and HMRC).
- This only applies in certain circumstances, so such requests for disclosure must be made in writing, providing details of the data subject, reason for disclosure, name of requesting officer and certification by a senior officer.
- A record must be kept of all such disclosures by services and a report made available to the DPO immediately upon request.

In all cases, if there are any concerns at all about an enquirer or their enquiry, information must not be given out, and the enquiry should be referred to the DPO.

## 15. Data sharing

Generally, the Council is not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

Services and officers might be approached and asked if the Council will enter into a **data sharing agreement** with another organisation. A data sharing agreement addresses arrangements whereby one organisation shares personal data with another organisation.

The Council will only share personal data it holds with third parties if:

1. they have a need to know the information for the purposes of providing the contracted services;
2. sharing the personal data complies with the Data Protection Principles;
3. the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
4. the transfer complies with any applicable cross border transfer restrictions; and
5. any necessary information sharing or data processing agreements are in place.

A statutory [Data sharing: a code of practice | ICO](#) in respect of data sharing arrangements between organisations has been issued by the ICO under [Section 121 of the Data Protection Act 2018](#).

The code explains how the 2018 Act applies to the sharing of personal data. It provides practical advice to organisations that share personal data and covers systematic data sharing arrangements as well as ad hoc or one-off requests to share personal data.

Data sharing agreements should be approved by the business manager for the service concerned and the negotiation and adjustment of the necessary legal documentation should be referred to the DPO and the Chief Officer of Legal and Democratic services, who will hold the signed completed agreements. The Council holds a record of all data sharing agreements.

## 16. Transferring Personal Information Outwith the UK or EEA

Both the UK GDPR and the Data Protection Act 2018 put restrictions on the transfer of personal data to countries outwith the UK. These restrictions are to ensure that such transfers do not undermine the level of protection for personal data. The Council will not transfer personal data outside the European Economic Area (EEA) unless this cannot be avoided.

1. The Council will only transfer data outside the UK and the EEA when it is satisfied that the party which will handle the data and the country it is processing it in will provide adequate safeguards for personal privacy. 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).
2. 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
3. The advice of the Data Protection Officer should be sought in relation to such issues.
4. If the Council need to transfer any personal information overseas in relation to a particular activity, this will be explained in the specific privacy statements relating to that function along with a description of the protective measures we have put in place to keep it secure.

## 17. Rights of individuals

All users must respect the rights of all individuals (data subjects), including employees and elected members. These include rights to:

- receive certain information about the Council's processing activities;
- request access to their personal data that we hold;
- prevent our use of their personal data for direct marketing purposes;
- ask us to erase personal data;
  - if it is no longer necessary in relation to the purposes for which it was collected or processed,
  - to rectify inaccurate data, or
  - to complete incomplete data;
- restrict processing in specific circumstances;
- challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
- object to decisions based solely on automated processing, including profiling;
- prevent processing that is likely to cause damage or distress to the data subject or anyone else;
- where processing is based on consent, withdraw consent to processing at any time;
- be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
- make a complaint to the ICO; and
- in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used, and machine-readable format.

The identity of an individual requesting data under any of the rights listed above should be verified before disclosing any personal information.

## 18. Product set

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

- Those listed under policies, procedures and guidance are the responsibility of the Data Protection team.
- Those listed under related products are the responsibility of other teams or services.

Product type	Product
Procedures	<ul style="list-style-type: none"> <li>▪ <a href="#">Data Breach Notification Form</a></li> <li>▪ <a href="#">Data Protection Breach and Incident Management Protocol</a></li> <li>▪ <a href="#">Data Protection Impact Assessment Template</a></li> <li>▪ <a href="#">Data protection procedures and guidance</a></li> <li>▪ <a href="#">Register of Data Sharing Agreements</a></li> </ul>
Guidance	<ul style="list-style-type: none"> <li>▪ <a href="#">DPIA and Lawful Bases</a></li> <li>▪ <a href="#">SAR Guidance</a></li> </ul>
Related products	<ul style="list-style-type: none"> <li>▪ <a href="#">Acceptable Use of IT Policy</a></li> <li>▪ <a href="#">Digital and IT Strategy</a></li> <li>▪ <a href="#">Discipline Policy</a></li> <li>▪ <a href="#">Information Asset Register</a></li> <li>▪ <a href="#">Information Security Policy</a></li> <li>▪ <a href="#">Records and Information Management Policy</a></li> <li>▪ <a href="#">Records Retention Schedule</a></li> <li>▪ <a href="#">Risk Management Strategy</a></li> <li>▪ <a href="#">Privacy notice</a></li> </ul>
Legislation, regulations, and government guidance	<ul style="list-style-type: none"> <li>▪ <a href="#">Councillors' Code of Conduct</a></li> <li>▪ <a href="#">Data Protection Act 2018</a> <ul style="list-style-type: none"> <li>▪ <a href="#">Schedule 1 of the Data Protection Act 2018</a></li> <li>▪ <a href="#">Section 121 of the Data Protection Act 2018</a></li> </ul> </li> <li>▪ <a href="#">ICO guidance on the UK General Data Protection Regulation</a> <ul style="list-style-type: none"> <li>▪ <a href="#">ICO Data Sharing Code of Practice</a></li> <li>▪ <a href="#">ICO guidance to organisations on the UK GDPR</a></li> <li>▪ <a href="#">ICO Special Category Data</a></li> </ul> </li> <li>▪ <a href="#">The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020</a></li> <li>▪ <a href="#">UK General Data Protection Regulation</a> <ul style="list-style-type: none"> <li>▪ <a href="#">Article 9 of the UK GDPR</a></li> <li>▪ <a href="#">Article 10 of the UK GDPR</a></li> </ul> </li> </ul>

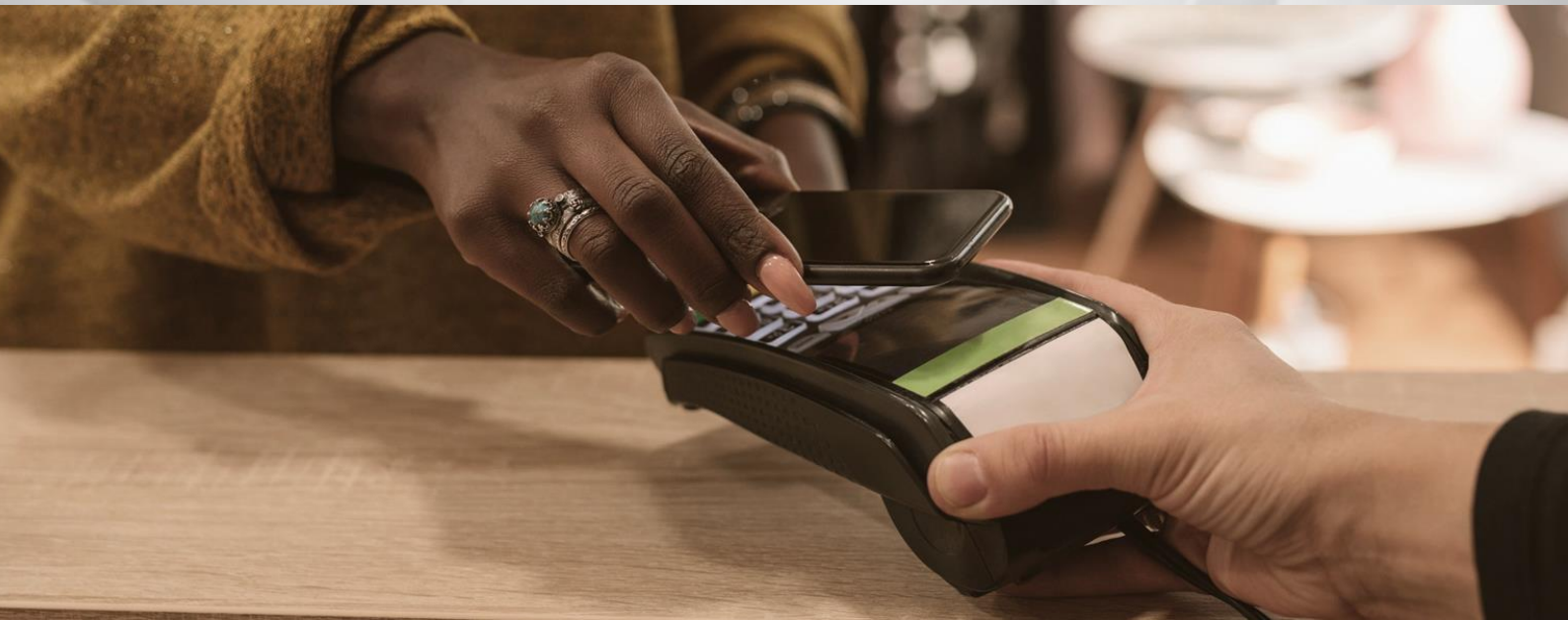
## Appendix 1: Glossary of terms

Term	Description
<b>The Act</b>	Data Protection Act 2018
<b>All Users</b>	All parties who have access to Council information including employees, elected members and third-party contractors and any other individuals or organisations who access Council information.
<b>Council Information</b>	Council information includes data, records, paper, and digital formats.
<b>Controller</b>	<p>The people or organisations who determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the data protection laws.</p> <p>The Council is the controller of all personal data used in its business.</p>
<b>Data Protection Laws</b>	The UK GDPR and the Act
<b>DPO</b>	Data Protection Officer
<b>DWP</b>	Department of Work and Pensions
<b>The UK GDPR</b>	UK General Data Protection Regulation
<b>HMRC</b>	Her Majesty's Revenue & Customs
<b>ICO</b>	Office of the Information Commissioner
<b>Personal Data</b>	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.
<b>Special Category Personal Data</b>	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.

Term	Description
<b>Processing</b>	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.
<b>Processor</b>	Any person who processes personal data on behalf of a controller such as the Council.  Council employees are excluded from this definition, but it could include suppliers which handle personal data on behalf of the Council, for example where the Council outsources IT, payroll, paper waste disposal, and mail shot / marketing services.
<b>SIRO</b>	Senior Information Risk Owner.

# **PAYMENT CARD DATA SECURITY POLICY**

**VERSION 2.0, MARCH 2026**



<b>Document control</b>			
<b>Title</b>	<b>Payment Card Data Security Policy</b>		
<b>Owner</b>	Chief Officer (Legal and Democratic)	<b>Contact</b>	<a href="mailto:InformationRiskAndAssuranceTeam@northlan.gov.uk">InformationRiskAndAssuranceTeam@northlan.gov.uk</a>
<b>Governance group</b>	Data Governance Board		
<b>Author</b>	Information Compliance Officer	<b>Contact</b>	<a href="mailto:InformationRiskAndAssuranceTeam@northlan.gov.uk">InformationRiskAndAssuranceTeam@northlan.gov.uk</a>

<b>Revision History</b>			
Number	Originator	Date review commenced	Revision description/record of change
2.0	Information Risk Manager	28 February 2025	Two-yearly review and change of writing style from second to third person.
1.0	Information Risk Manager	None	New policy.

<b>Document Approvals</b>			
Number	Governance group	Date approval granted	Date approval to be requested (if document still draft)
2.0	Policy and Strategy Committee		19 March 2026
1.0	Policy and Strategy Committee	08 June 2023	

<b>Consultation Record (for most recent update)</b>		
<b>Status of document consulted upon</b>	Stakeholders consulted between 11 March 2025 and 22 December 2025.	
<b>Stakeholders consulted and dates</b>	Data Management Team Technology Strategy Manager Data Governance Board PCI DSS Governance Board Corporate Management Team	11 March 2025 11 March 2025 26 March 2025 03 April 2025 22 December 2025

<b>Strategic Alignment</b>
<p><b>Plan for North Lanarkshire</b> Improving North Lanarkshire’s resource base – Build a workforce for the future capable of delivering on our priorities and shared ambition.</p>
<p><b>Digital and IT Strategy</b> 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.</p> <p>The Payment Card Data Security Policy is one of these. It supports the strategy by providing a safe framework for processing, storing and transmitting payment card and cardholder details in line with mandatory worldwide standards.</p>

<b>Next review date</b>	
<b>Review date</b>	March 2028

# Contents

1	Introduction .....	1
2	Purpose .....	1
3	Scope.....	3
4	Governance.....	3
5	Policy compliance.....	4
6	Policy objectives .....	5
7	Security controls.....	5
7.1	Managing risk .....	5
7.2	Managing information .....	6
7.3	Operational security .....	6
7.4	Physical security.....	7
7.5	Third-party supplier and service provider security.....	8
7.6	Training and awareness.....	9
8	Product set.....	9
	Appendix A: Payment card data handling roles and responsibilities .....	11

# 1 Introduction

North Lanarkshire Council (the Council) takes credit and debit card payments for a range of goods and services – such as theatre tickets, special uplifts, council tax and housing rents. The Council must take card payments in a way that protects it and its customers from data breaches and fraud.

This policy sets out how the Council – and anyone who operates on its behalf to deliver or supply services – process credit and debit card payments securely in line with the Payment Card Industry Data Security Standard (PCI-DSS). Managed by the [Payment Card Industry Security Standards Council](#), this is a mandatory information security standard that applies worldwide to every organisation that stores, processes, or transmits cardholder data. It helps:

- reduce the likelihood of credit and debit card fraud;
- protect the processing, storage, and transmission of card and cardholder details; and
- secure how the Council handles data and its exposure to compromise.

The Council uses the following **payment channels**.

1. **Online** – self-service; customers make payments through websites and web services.
2. **Point-of-sale payment card machine** – face to face; customers pay at a Council facility.
3. **Telephone** – remote and self-service; customers speak to agents over the phone and make payments using an automated system.

---

**PCI-DSS is mandatory.**

**The consequences of non-compliance include financial penalties, no longer being allowed to process card payments, loss of revenue, and reputational damage.**

---

## 2 Purpose

This policy provides a framework to effectively protect the security of all card payments the Council receives and processes.

It makes sure the Council

- handles all payment card data and cardholder details securely, and
- complies with all PCI-DSS requirements.

In doing so, it balances the benefits and risks of processing card payments, in line with the three core principles of information security – known as the CIA triad.

### Confidentiality

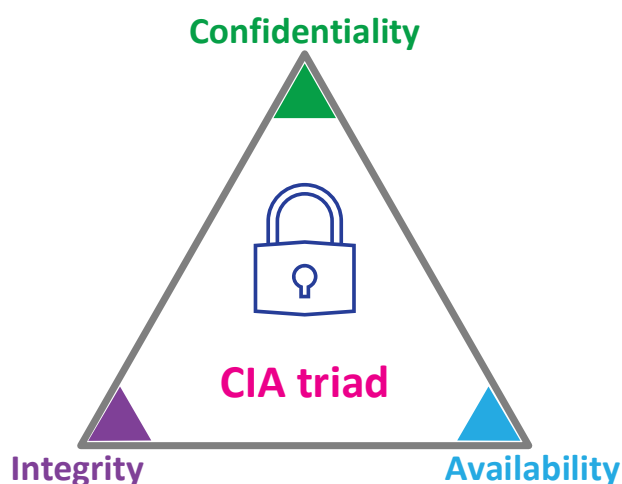
Only those who should see it, do see it.

### 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 processing information via card payments at the **OFFICIAL-SENSITIVE** 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](#)
  - [Information and Cyber 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.
- The [Information Classification and Handling Security Standard](#) – how to classify and handle information while safeguarding its confidentiality, integrity and availability.
- 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 payment card data security, including the following.

1. All IT assets – systems, services, and devices – that the Council uses to store, process, transmit or receive payment card data and cardholder details – including how it specifies, designs, develops, installs, operates, connects, uses, and decommissions them.
2. All information assets relating to card payments – 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 hosted within the Council IT network and on cloud-based services.
  - **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.
3. Every authorised person who processes, accesses or otherwise handles payment card data and cardholder details on the Council's behalf. This includes all employees, Councillors, 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 Compliance Group** (formerly Data Management Team), the **Data Governance Board** then the **PCI DSS Governance Board** – as **key stakeholders** – oversee its review and consider its contents before referring it on for approval. The **Chief Officer of Legal and Democratic** – 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.
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 every two years, with other reviews when needed. For example, following a critical security incident, new legislation, a significant threat, an audit action.
4. Report to management teams, governance and working groups, committees and scrutiny panels.

## 5 Policy compliance

Every person who processes card payments and or handles cardholder data 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:

1. only using the data for its intended purpose – unless authorised to do otherwise;
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
- Chief Officer of Finance and Technology
- Data Governance Board
- Senior Information Risk Owner
- Technology Strategy Manager
- Third-party suppliers and service providers
- Corporate Management Team
- PCI DSS Governance Board
- Data Management 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 payment card data 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 card data, including the IT infrastructure and systems that to store, process and transmit it.
2. Show key stakeholders – such as elected members, residents, customers and service users – that the Council treats and protects cardholder data in line with its value and sensitivity.
3. Help everyone who processes card payments and or handles cardholder data on behalf of the Council 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. Promote compliance with all relevant legislation and regulations.
6. Align processes for payment card data security standards, procedures, and guidance with the Council's Security Standards Framework.

## 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 risks to payment card data.

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 implements security operational procedures and user guidance.
5. Produces mandatory training for all employees and targeted training for employees who process payment card data.
6. 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, Information and Cyber 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](#) outlines how to classify, protectively mark, and handle sensitive information. Payment card data is **OFFICIAL-SENSITIVE – PERSONAL**.
2. **Records retention:** The [Records Retention Schedule](#) specifies
  - 2.1. how long to keep payment card data, and
  - 2.2. how to securely dispose of it, including the following.
    - Securely destroy any sensitive card data when no longer needed so that it's unrecoverable.
    - Securely delete all digital data – on all systems and services – when no longer needed.
    - Destroy all hard copies of cardholder data when there's no longer a valid business reason to keep it.

## 7.3 Operational security

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

1. **Compliance:** Legislation and regulations, data sharing arrangements and contractual obligations.
2. **Access controls** to manage and restrict access to cardholder data, including –
  - 2.1. **User access** including using permissions and privileges.

- Clearly defined job functions that must access cardholder data.
  - Restrict and pre-authorise all access to cardholder data – including the long card number, personal information and business data – to only those who have a legitimate business need to view it. Don't give anyone else access to this data.
- 2.2. **Access to IT systems and services** including system controls to protect against unauthorised access, service disruption, data breach and data loss.
- 2.3. **Third-party access** as defined in the [Code of Connection procedures](#).
3. **Stored data:** Protect cardholder data against any unauthorised use.
- 3.1. **Never store the following data** on any information asset or device.
- **Track data** – that is, the contents of the payment card magnetic stripe.
  - **CVV or CVC** (card verification value or code) – commonly known as the **security code**, this is a three or four-digit number usually on the back of the payment card.
  - **PIN** (personal identification number) – that the cardholder types into the machine.
  - **PIN block** – used to send a new PIN, it is encrypted and includes an authentication code.
- 3.2. **Don't display full long card numbers.**
- Only ever display the card's first six digits and the last four digits of the permanent account number (commonly known as the long card number).
  - Don't display the full number onscreen unless there's a need to show it all.
4. **Data in transit:** Protect cardholder data when transmitting it digitally or transporting it physically.
- 4.1. Never send any card details – full long card number, track data, security code, PIN, PIN block – across or outside the Council IT network using messaging services such as email and chat, or any other unencrypted or unauthorised system or service.
- 4.2. If there is a business reason to transmit or transport cardholder data, the appropriate manager must authorise it first. Use the following safety controls.
- Digital – Use a [strong encryption](#) mechanism when using email or another digital system or service.
  - Physical – log and inventory the data before leaving the premises. Only use secure courier services. Monitor the shipment status through to delivery confirmation.
5. **Information security incidents:** The [Information Security Incident Management Procedure](#) and the [Data Protection Breach and Incident Management Protocol](#) explain how to react to actual and suspected security incidents and data breaches. The Cardholder Data Breach Incident Response Plan details how to handle incidents involving cardholder data breaches. This is a restricted access document.

## 7.4 Physical security

Apply the following **physical controls for payment card data and machines** to restrict access to sensitive information and prevent unauthorised individuals from accessing it. This includes all types of information assets as detailed in the [scope](#) of this document.

1. Only those authorised to do so can handle and distribute information assets that contain sensitive data. They must do this in a secure manner.
2. Trusted employees must always escort visitors when in areas that hold sensitive cardholder information.
3. Keep a list of all payment card machines
  - 3.1. including the make, model, location, serial number or other unique identifier, and
  - 3.2. update the list whenever anyone adds, removes or relocates a machine; and
4. Routinely check payment card machine surfaces to detect if they've been tampered with or swapped out with an unauthorised machine for fraudulent purposes.
5. Always check and verify the identity of anyone claiming to be from an authorised third party who wants to install, replace, repair or run maintenance tasks on, or otherwise access Council payment card machines.
6. Use lockable storage containers – clearly marked for secure and sensitive disposal – to store all physical cardholder data awaiting destruction. Restrict access to these containers.

## 7.5 Third-party supplier and service provider security

The Council uses third-party suppliers and service providers to process card payments, subject to the following mandatory security controls.

### 1. The Council must do the following.

- 1.1. Use established [corporate procurement processes](#), including formal due diligence, before engaging with a service provider.
- 1.2. Formally monitor the service provider's PCI DSS compliance status.
- 1.3. Keep a list of all third-party suppliers and service providers the Council shares cardholder data with.

### 2. Third-party suppliers and service providers the Council contracts to operate on its behalf by providing services and solutions.

- 2.1. Are contractually obliged to
  - comply with PCI-DSS, and
  - include a specific agreement that they are responsible for cardholder data they hold.
- 2.2. 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

The [Information and Cyber Security Policy](#) details how the Council uses training and awareness to help manage risk. This includes the following.

1. **Mandatory training modules** on [LearnNL](#) covering the core elements of information governance – data protection, information and cyber security, and records and Information management.
2. **Awareness raising activities** to promote information and cyber security, share information and build knowledge.
3. **Specific training on payment card machines** for everyone who uses them, including how to
  - safely use them,
  - properly handle cardholder details, and
  - identify and report suspicious behaviour and possible tampering.

## 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.
- Those listed under legislation, regulations, and government guidance are the responsibility of other agencies.

Product type	Product
Strategies	<ul style="list-style-type: none"><li>▪ <a href="#">Digital and IT Strategy</a></li><li>▪ <a href="#">Risk Management Strategy</a></li></ul>
Policies	<ul style="list-style-type: none"><li>▪ <a href="#">Acceptable Use of IT Policy</a></li><li>▪ <a href="#">Data Protection Policy</a></li><li>▪ <a href="#">Discipline Policy</a></li><li>▪ <a href="#">Information and Cyber Security Policy</a></li><li>▪ <a href="#">Records and Information Management Policy</a></li></ul>
Frameworks	<ul style="list-style-type: none"><li>▪ <a href="#">Security Standards Framework</a></li></ul>
Standards	<ul style="list-style-type: none"><li>▪ <a href="#">Information Classification and Handling Security Standard</a></li></ul>
Procedures	<ul style="list-style-type: none"><li>▪ <a href="#">Code of Connection procedures</a></li><li>▪ <a href="#">Data Protection Breach and Incident Management Protocol</a></li><li>▪ <a href="#">Information Security Incident Management Procedure</a></li></ul>

Product type	Product
Related products	<ul style="list-style-type: none"> <li>▪ <a href="#">Records retention schedule</a></li> <li>▪ <a href="#">Corporate procurement intranet document library</a></li> <li>▪ <a href="#">LearnNL</a></li> </ul>
Legislation, regulations, and government guidance	<ul style="list-style-type: none"> <li>▪ <a href="#">Computer Misuse Act 1990: GOV.UK</a></li> <li>▪ <a href="#">Copyright, Designs and Patents Act 1988: GOV.UK</a></li> <li>▪ <a href="#">Cyber Resilient Scotland: strategic framework – Public Sector Action Plan: GOV.SCOT</a></li> <li>▪ <a href="#">Data Protection Act 2018: GOV.UK</a></li> <li>▪ <a href="#">General Data Protection Regulations</a></li> <li>▪ <a href="#">Government Security Classification Policy: GOV.UK</a></li> <li>▪ <a href="#">Government Security Classifications: GOV.UK</a></li> <li>▪ <a href="#">Payment Card Industry Data Security Standard: PCI</a></li> <li>▪ <a href="#">Payment Card Industry Security Standards Council: PCI</a></li> <li>▪ <a href="#">Public Bodies (Joint Working) (Scotland) Act 2014: GOV.UK</a></li> <li>▪ <a href="#">Public Records (Scotland) Act 2011: GOV.UK</a></li> <li>▪ <a href="#">Public Services Network Connection Compliance: GOV.UK</a></li> <li>▪ <a href="#">Strong encryption: PCI</a></li> </ul>

# Appendix A: Payment card data handling roles and responsibilities

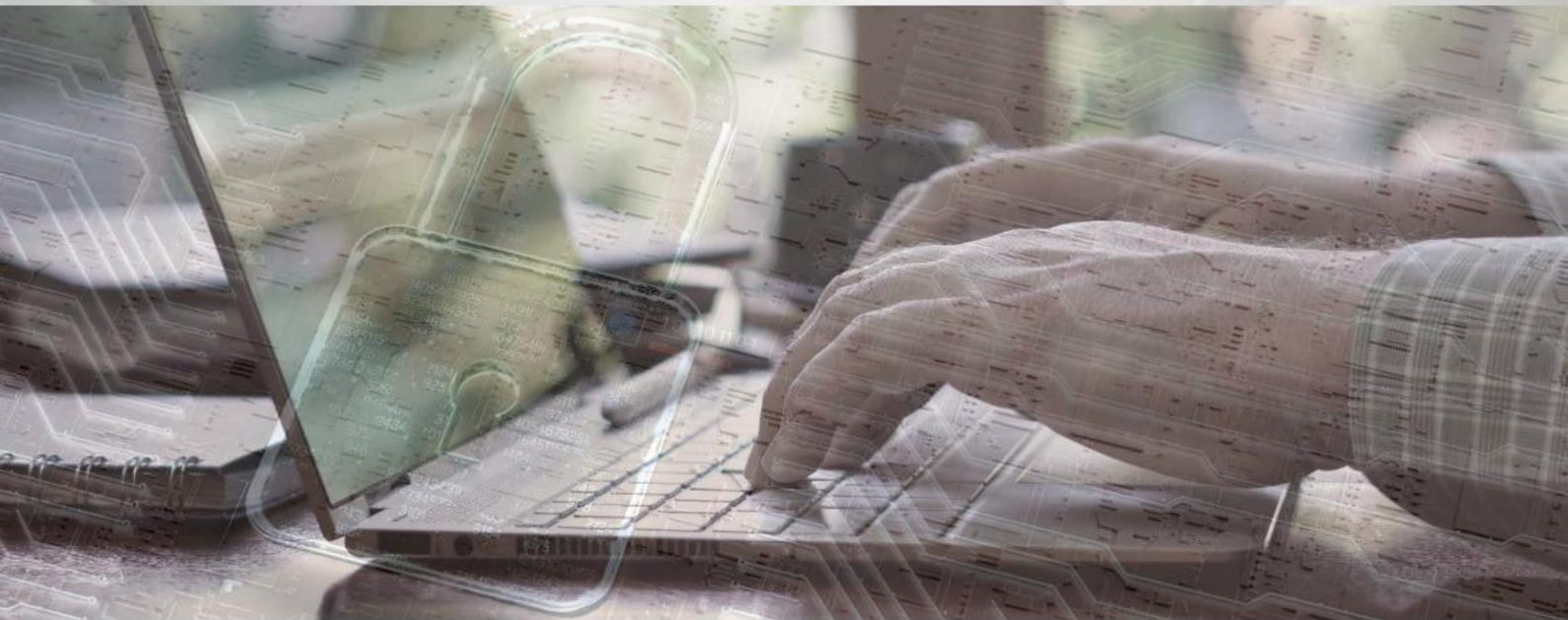
Role	Responsibilities
<p><b>Chief Executive</b> of North Lanarkshire Council.</p>	<ul style="list-style-type: none"> <li>▪ Overall accountability for the protection of information the Council owns and processes.</li> </ul>
<p><b>Chief Officer of Finance and Technology</b> The Council's subject matter expert on financial systems and solutions.</p>	<ul style="list-style-type: none"> <li>▪ Overall accountability for protecting financial data and making sure financial systems, devices, and processes comply with PCI DSS. This incorporates the annual PCI attestation of compliance which includes reviewing information security policies for currency and accuracy.</li> <li>▪ Accountable for putting in place policy, standards, and guidance in relation to financial solutions.</li> </ul>
<p><b>Senior Information Risk Owner (SIRO)</b> The Chief Officer Legal and Democratic has this role.</p>	<ul style="list-style-type: none"> <li>▪ Make sure the Council protects both its information, and its information storage facilities and processing systems.</li> <li>▪ Accountable for information and cyber security governance.</li> </ul>
<p><b>Corporate Management Team</b> Members are the Chief Executive, Depute Chief Executive, SIRO, and Chief Officers.</p>	<ul style="list-style-type: none"> <li>▪ Sign off on information and cyber security controls and practices.</li> <li>▪ Consider reports on the effectiveness of information and cyber security practices.</li> </ul>
<p><b>PCI DSS Governance Board</b> A senior officer group with ongoing responsibility for PCI DSS.</p>	<ul style="list-style-type: none"> <li>▪ Provide executive management oversight of Council activities to make sure the Council complies with PCI DSS.</li> </ul>
<p><b>Data Governance Board</b> A senior officer group of business information owners and subject matter experts from all services. Chaired by the SIRO.</p>	<ul style="list-style-type: none"> <li>▪ Assure robust information governance of this policy.</li> <li>▪ Consider revisions before passing to the Policy and Strategy Committee for approval.</li> </ul>

Role	Responsibilities
<p><b>Data Management Compliance Group</b> An officer group from all services with responsibility for business information including processes and IT systems.</p>	<ul style="list-style-type: none"> <li>▪ Individual members must make sure their service complies with this policy and related standards, procedures and guidance.</li> <li>▪ Collectively the team: <ul style="list-style-type: none"> <li>▪ oversees the review of this policy; and</li> <li>▪ agrees revisions before passing to the Data Governance Board to consider.</li> </ul> </li> </ul>
<p><b>Information Risk Manager</b> Lead subject matter expert on information and cyber security risk and assurance.</p>	<ul style="list-style-type: none"> <li>▪ Co-ordinate and monitor activities to manage the Council's information risk posture, including: <ul style="list-style-type: none"> <li>▪ network controls, specialist systems, and privileged utility programs to protect the IT infrastructure; and</li> <li>▪ mandatory training and awareness raising.</li> </ul> </li> <li>▪ Produce and promote this policy and related standards, procedures and guidance.</li> </ul>
<p><b>Technology Strategy Manager</b> Responsible for managing the Council's IT infrastructure.</p>	<ul style="list-style-type: none"> <li>▪ Implement, manage and monitor technical security measures, in line with appropriate security standards to protect the Council's <ul style="list-style-type: none"> <li>▪ IT infrastructure,</li> <li>▪ IT assets, and</li> <li>▪ digital information assets managed or stored by Technology and Digital Strategy services.</li> </ul> </li> </ul>
<p><b>All managers</b> Anyone responsible for managing a function or group of people within the Council. This includes information, IT asset and product owners.</p>	<ul style="list-style-type: none"> <li>▪ Make sure processes and security controls are in place to manage information effectively.</li> <li>▪ Make sure staff members: <ul style="list-style-type: none"> <li>▪ understand their compliance responsibilities and the consequences of non-compliance;</li> <li>▪ follow policies, standards, procedures and guidance; and</li> <li>▪ keep up to date with mandatory training.</li> </ul> </li> </ul>

Role	Responsibilities
<p><b>Third-party suppliers and service providers</b></p> <p>All third-party organisations and their individual employees that the Council contracts to operate on its behalf by providing services and solutions.</p>	<ul style="list-style-type: none"> <li>▪ Understand their compliance responsibilities and the consequences of non-compliance, as contractually agreed.</li> </ul>
<p><b>Everyone</b></p> <p>As per the <a href="#">scope</a>, every person who processes card payments and or handles cardholder data on behalf of the Council.</p>	<ul style="list-style-type: none"> <li>▪ Follow policies, standards, procedures and guidance, and process card payments and protect cardholder data in line with them.</li> <li>▪ Keep up to date with: <ul style="list-style-type: none"> <li>▪ mandatory training; and</li> <li>▪ general awareness communications.</li> </ul> </li> </ul>

# **INFORMATION AND CYBER SECURITY POLICY**

**VERSION 5.0, MARCH 2026**



<b>Document control</b>			
<b>Title</b>	<b>Information and Cyber Security Policy</b>		
<b>Owner</b>	Chief Officer (Legal and Democratic)	<b>Contact</b>	<a href="mailto:InformationRiskAndAssuranceTeam@northlan.gov.uk">InformationRiskAndAssuranceTeam@northlan.gov.uk</a>
<b>Governance group</b>	Data Governance Board		
<b>Author</b>	Information Compliance Officer	<b>Contact</b>	<a href="mailto:InformationRiskAndAssuranceTeam@northlan.gov.uk">InformationRiskAndAssuranceTeam@northlan.gov.uk</a>

<b>Revision history</b>			
<b>Number</b>	<b>Originator</b>	<b>Date review commenced</b>	<b>Revision description/record of change</b>
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.

<b>Document approvals</b>			
<b>Number</b>	<b>Governance group</b>	<b>Date approval granted</b>	<b>Date approval to be requested</b> (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	

<b>Consultation record (for most recent update)</b>		
<b>Status of document consulted upon</b>	Stakeholders consulted between 11 March 2025 and 22 December 2025.	
<b>Stakeholders consulted and dates</b>	Data Management Team Technology Strategy Manager Data Governance Board Corporate Management Team	11 March 2025 11 March 2025 26 March 2025 22 December 2025

<b>Strategic alignment</b>
<b>Plan for North Lanarkshire</b> 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**

<b>Review date</b>	March 2028
--------------------	------------

# Contents

1	Introduction .....	1
2	Purpose .....	2
3	Scope.....	3
4	Governance.....	3
5	Policy compliance.....	4
6	Policy objectives .....	5
7	Security controls.....	6
7.1	Managing risk .....	6
7.2	Managing information .....	6
7.3	Operational security .....	7
7.4	Cyber security.....	8
7.5	Third-party supplier and service provider security.....	9
7.6	Training and awareness.....	10
8	Product set.....	11
	Appendix A: Information and cyber security roles and responsibilities .....	13
	Appendix B: Cyber Security Framework core functions and categories .....	15

# 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

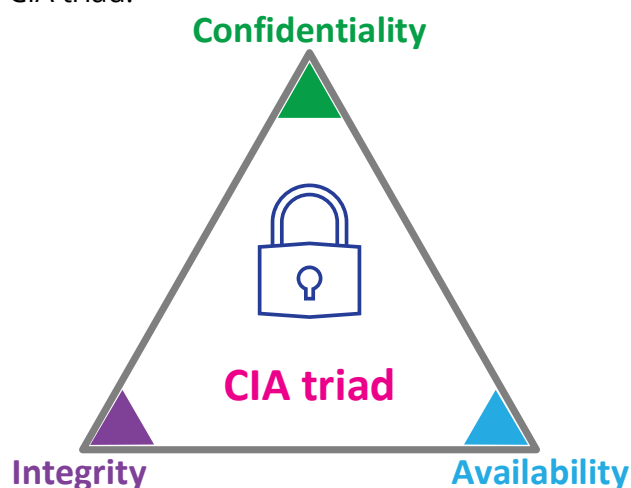
Only those who should see it, do see it.

### 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 and Democratic** – 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.
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 every two years, with other reviews when needed. For example, following a critical security incident, new legislation, a significant threat, or an audit action.
4. 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.

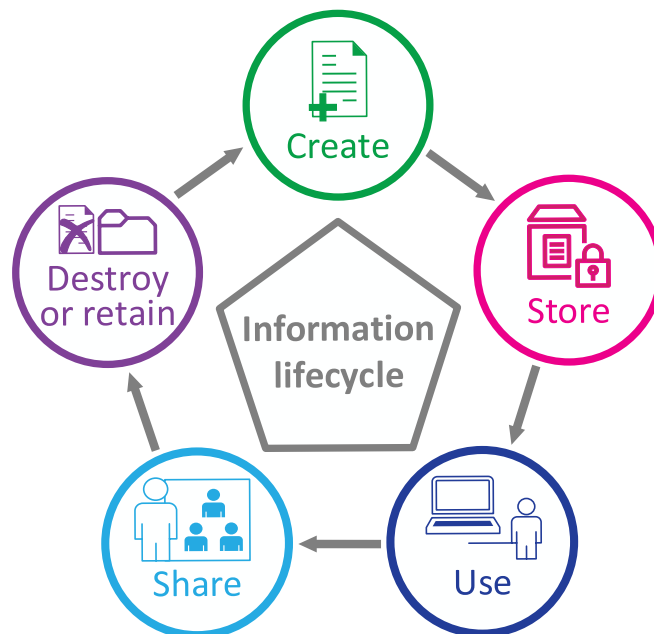
### User guidance to help manage information securely

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.
- Those listed under legislation, regulations, and government guidance are the responsibility of other agencies.

Product type	Product
Strategies	<ul style="list-style-type: none"> <li>▪ <a href="#">Digital and IT Strategy</a></li> <li>▪ <a href="#">Risk Management Strategy</a></li> </ul>
Policies	<ul style="list-style-type: none"> <li>▪ <a href="#">Acceptable Use of IT Policy</a></li> <li>▪ <a href="#">Data Protection Policy</a></li> <li>▪ <a href="#">Discipline Policy</a></li> <li>▪ <a href="#">Payment Card Data Security Policy</a></li> <li>▪ <a href="#">Records and Information Management Policy</a></li> </ul>
Frameworks	<ul style="list-style-type: none"> <li>▪ <a href="#">Corporate Procurement model</a></li> <li>▪ <a href="#">Project Management Framework</a></li> <li>▪ <a href="#">Security Standards Framework</a></li> </ul>
Standards	<ul style="list-style-type: none"> <li>▪ <a href="#">Code of Conduct for Chief Officers</a></li> <li>▪ <a href="#">Employee Code of Conduct</a></li> <li>▪ <a href="#">IT Systems Resiliency and Disaster Recovery Standard</a></li> <li>▪ <a href="#">Information Classification and Handling Security Standard</a></li> </ul>
Procedures	<ul style="list-style-type: none"> <li>▪ <a href="#">Code of Connection procedures</a></li> <li>▪ <a href="#">Data Protection Breach and Incident Management Protocol</a></li> <li>▪ <a href="#">Information Security Incident Management Procedure</a></li> </ul>
Guidance	<ul style="list-style-type: none"> <li>▪ <a href="#">Business continuity guidance</a></li> <li>▪ <a href="#">Email security guidance</a></li> <li>▪ <a href="#">Intranet document library</a></li> <li>▪ <a href="#">IT Authentication (Password) and Secure Access User Guidance</a></li> <li>▪ <a href="#">Purchasing Cloud-based Services Cyber Security Guidance</a></li> <li>▪ <a href="#">Quick guide to information handling rules</a></li> <li>▪ <a href="#">Quick guide to remote working security</a></li> <li>▪ <a href="#">SCAM checklist</a></li> <li>▪ <a href="#">Viva Engage community page</a></li> </ul>

Product type	Product
Related products	<ul style="list-style-type: none"> <li>▪ <a href="#">Council news on the intranet</a></li> <li>▪ <a href="#">Information Asset Register</a></li> <li>▪ <a href="#">LearnNL</a></li> <li>▪ <a href="#">Records Retention Schedule</a></li> </ul>
Legislation, regulations, and government guidance	<ul style="list-style-type: none"> <li>▪ <a href="#">Computer Misuse Act 1990: GOV.UK</a></li> <li>▪ <a href="#">Copyright, Designs and Patents Act 1988: GOV.UK</a></li> <li>▪ <a href="#">Councillors' Code of Conduct</a></li> <li>▪ <a href="#">Cyber Resilient Scotland: strategic framework – Public Sector Action Plan: GOV.SCOT</a></li> <li>▪ <a href="#">Cyber Security Framework: NIST</a></li> <li>▪ <a href="#">Data Protection Act 2018: GOV.UK</a></li> <li>▪ <a href="#">General Data Protection Regulations</a></li> <li>▪ <a href="#">Government Security Classifications: GOV.UK</a></li> <li>▪ <a href="#">Government Security Classification Policy: GOV.UK</a></li> <li>▪ <a href="#">Public Bodies (Joint Working) (Scotland) Act 2014: GOV.UK</a></li> <li>▪ <a href="#">Public Records (Scotland) Act 2011: GOV.UK</a></li> <li>▪ <a href="#">Payment Card Industry Data Security Standard: PCI</a></li> <li>▪ <a href="#">Public Services Network Connection Compliance: GOV.UK</a></li> </ul>

# Appendix A: Information and cyber security roles and responsibilities

Role	Responsibilities
<p><b>Chief Executive</b> of North Lanarkshire Council.</p>	<ul style="list-style-type: none"> <li>▪ Overall accountability for the protection of information the Council owns and processes.</li> </ul>
<p><b>Senior Information Risk Owner (SIRO)</b> The Chief Officer of Legal and Democratic has this role.</p>	<ul style="list-style-type: none"> <li>▪ Make sure the Council protects both its information, and its information storage facilities and processing systems.</li> <li>▪ Accountable for information and cyber security governance.</li> </ul>
<p><b>Corporate Management Team</b> Members are the Chief Executive, Depute Chief Executive, SIRO, and Chief Officers.</p>	<ul style="list-style-type: none"> <li>▪ Sign off on information and cyber security controls and practices.</li> <li>▪ Consider reports on the effectiveness of information and cyber security practices.</li> </ul>
<p><b>Data Governance Board</b> A senior officer group of business information owners and subject matter experts from all services. Chaired by the SIRO.</p>	<ul style="list-style-type: none"> <li>▪ Assure robust information governance of this policy.</li> <li>▪ Consider revisions before passing to the Policy and Strategy Committee for approval.</li> </ul>
<p><b>Data Management and Compliance Group</b> An officer group from all services with responsibility for business information including processes and IT systems.</p>	<ul style="list-style-type: none"> <li>▪ Individual members must make sure their service complies with this policy and related standards, procedures and guidance.</li> <li>▪ Collectively the group:               <ul style="list-style-type: none"> <li>▪ oversees the review of this policy; and</li> <li>▪ agrees revisions before passing to the Data Governance Board to consider.</li> </ul> </li> </ul>
<p><b>Information Risk Manager</b> Lead subject matter expert on information and cyber security risk and assurance management.</p>	<ul style="list-style-type: none"> <li>▪ Co-ordinate and monitor activities to manage the Council's information risk posture, including:               <ul style="list-style-type: none"> <li>▪ network controls, specialist systems, and privileged utility programs to protect the IT infrastructure; and</li> <li>▪ mandatory training and awareness raising.</li> </ul> </li> <li>▪ Produce and promote this policy and related standards, procedures and guidance.</li> </ul>

Role	Responsibilities
<p><b>Technology Strategy Manager</b> Responsible for managing the Council IT infrastructure.</p>	<ul style="list-style-type: none"> <li>▪ Implement, manage and monitor technical security measures, in line with appropriate security standards to protect the Council's <ul style="list-style-type: none"> <li>▪ IT infrastructure,</li> <li>▪ IT assets, and</li> <li>▪ digital information assets managed or stored by Technology and Digital Strategy services.</li> </ul> </li> </ul>
<p><b>All managers</b> Anyone responsible for managing a function or group of people within the Council. This includes information, IT asset and product owners.</p>	<ul style="list-style-type: none"> <li>▪ Make sure processes and security controls are in place to manage information effectively.</li> <li>▪ Make sure staff members: <ul style="list-style-type: none"> <li>▪ understand their compliance responsibilities and the consequences of non-compliance;</li> <li>▪ follow policies, standards, procedures and guidance; and</li> <li>▪ keep up to date with mandatory training.</li> </ul> </li> </ul>
<p><b>Third-party suppliers and service providers</b> All third-party organisations and their individual employees that the Council contracts to operate on its behalf by providing services and solutions.</p>	<ul style="list-style-type: none"> <li>▪ Understand their compliance responsibilities and the consequences of non-compliance, as contractually agreed.</li> </ul>
<p><b>Everyone</b> As per the <a href="#">scope</a>, 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.</p>	<ul style="list-style-type: none"> <li>▪ Follow policies, standards, procedures and guidance, and protect Council information, devices, information storage facilities and processing systems in line with them.</li> <li>▪ Keep up to date with: <ul style="list-style-type: none"> <li>▪ mandatory training; and</li> <li>▪ general awareness communications.</li> </ul> </li> </ul>

# 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

# Records and Information Management Policy

Version 6.0, 05 November 2025

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.

**LIVE  
LEARN  
WORK  
INVEST  
VISIT**

# Document control

<b>Title</b>	Records and Information Management Policy		
<b>Governance group</b>	Data Governance Board		
<b>Owner</b>	Rachel Blair, Senior Information Risk Officer	<b>Contact</b>	<a href="mailto:Blairr@northlan.gov.uk">Blairr@northlan.gov.uk</a>
<b>Author</b>	Fiona Hughes, Corporate Records Manager	<b>Contact</b>	<a href="mailto:hughesfi@northlan.gov.uk">hughesfi@northlan.gov.uk</a>

## Revision history

Version	Originator	Review start date	Revision description and record of change
6.0	Fiona Hughes	21 July 2025	Bi-annual review.
5.0	Fiona Hughes		Bi-annual review.
4.0	Fiona Hughes	26 March 2021	Full review.
3.0	Fiona Hughes	15 January 2019	Bi-annual review.
2.0	Fiona Hughes	15 November 2016	Bi-annual review process. Revised in line with Records Management Plan.
1.0	Marcia Jarnell	25 July 2014	Combination of Record Management and Information Management policies.

## Document approvals

Version	Governance group	Date approved	Date approval requested (if document still in draft)
6.0			05 Nov 2025
5.0	Business and Digital Delivery Board	08 June 2023	
4.0	Policy and Strategy Committee	03 June 2021	
3.0	Policy and Strategy Committee	10 June 2020	
2.0	Policy and Resources Committee	21 June 2017	
1.0	Policy and Resources Committee	18 September 2014	

## Consultation record (for most recent update)

<b>Consultation status</b>	Stakeholders consulted between 21 October 2025 and 05 November 2025	
<b>Stakeholders consulted and dates</b>	Data Management & Compliance Group	21 October 2025

## 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 Records and Information Management Policy is one of these. It supports the strategy by providing a framework for good record keeping practices making sure records are managed effectively and efficiently, and the Council complies with its statutory and regulatory obligations.

## Next review date

<b>Review Date</b>	01 May 2027
--------------------	-------------

# Contents

1. Introduction.....	4
2. Purpose .....	4
3. Scope .....	5
4. Governance.....	5
5. Objectives.....	5
6. Records and information lifecycle management .....	6
7. Capture and control of records .....	6
8. Storage of records.....	8
9. Access to records .....	8
10. Audit trail.....	8
11. Retention and disposal .....	9
12. Transfer to archive .....	9
13. Destructions .....	10
14. Responsibilities .....	10
15. Product set.....	11
Appendix 1: Glossary of terms.....	12

# 1. Introduction

Information and records are an essential corporate asset without which we would be unable to carry out our functions, activities and transactions, meet the needs of our stakeholders, provide evidence of our activities and ensure legislative compliance.

**Records management** is the systematic control of an organisation's records, throughout their lifecycle, to meet operational business needs, statutory and fiscal requirements and community expectations.

The benefits of implementing records management systems and processes include:

1. Improved business efficiency through reduced time spent searching for information;
2. demonstration of transparency and accountability for all actions;
3. the maintenance of corporate memory and evidence of Council business and decision-making;
4. the creation of modern working environments and identification of opportunities for office rationalisation and hybrid working;
5. risk management in terms of ensuring and demonstrating compliance with all legal, regulatory and statutory obligations, and
6. the meeting of stakeholder expectations through the provision of good quality services.

---

**North Lanarkshire Council recognises the importance of effective records management in supporting its core functions, providing authentic and reliable evidence of Council business, and documenting historical and cultural activity within North Lanarkshire.**

---

## 2. Purpose

This policy demonstrates that the Council considers records and information to be a vital corporate asset and is committed to managing them lawfully and in compliance with current standards of professional practice. It acts as a mandate for the support and delivery of records management guidance, training, procedures and initiatives across the organisation.

The [Public Records \(Scotland\) Act 2011](#) requires the Council to produce a [Records Management Plan](#) which sets out its proper arrangements for the effective management of all public records. The act defines public records as records created by, on behalf of, or in the possession of, the authority or a contractor, in carrying out the functions of the Council. Having a records management policy statement fulfils one of the mandatory elements of this plan.

## 3. Scope

This policy is applicable to all records created or managed by North Lanarkshire Council and North Lanarkshire Licensing Board for the purpose of performing Council functions, and applies to Council records in all formats, whether accessed on Council premises or via mobile or home-working equipment. It also applies to records managed on Council systems on behalf of North Lanarkshire Integration Joint Board.

The policy applies to all staff, workers, elected members, clients, suppliers, third party contractors and any other individuals or organisations who carry out functions on behalf of the Council.

## 4. Governance

This policy forms part of a suite of documents that form part of the [Digital and IT Strategy](#).

The **Business and Digital Delivery Board** has **approval** authority for, and oversight of, this policy. The **Data Management Compliance Group** – as **key stakeholders** – oversee its review and consider its contents before referring it on for approval. The **Chief Officer of Legal and Democratic** – as the Council's Senior Information Risk Owner – is **accountable** for its governance. The **Records and Archives team** is **responsible** for the following activities:

1. Produce, publish and promote this policy. Provide guidance on how to apply and comply with this policy through standards, procedures and guidance notes as referred to within the policy.
2. Review every two years, with other reviews when needed. For example, following new legislation, new guidance or an audit action.
3. Report to management teams, governance and working groups, committees and scrutiny panels.

## 5. Objectives

The objectives of this policy are to:

- Provide a **framework** for good record keeping practices within the Council, ensuring that records are managed effectively and efficiently, and that the Council complies with its statutory and regulatory obligations.
- Develop and encourage a **working culture** that recognises and acknowledges the benefits of effective records management.
- Ensure a **corporate approach** to the management of the Council's records as a corporate resource.
- Define **responsibilities** for records management throughout the Council.
- Ensure that Council records are **reliable, authentic** and have **integrity**.

- Ensure that records are **retrievable** as required but also **secure** to prevent unauthorised access, alteration or destruction.
- Ensure **lawful management** of records that include **personal data**. Support **public rights of access** to information. Ensure that **records of long-term value are identified and preserved as archives** within the collections of the Council.

## 6. Records and information lifecycle management

The lifecycle of a record comprises the following:

- initial creation by the Council or receipt from a third party;
- maintenance and use, including sharing and audit; and
- disposal through confidential destruction or preservation in the Council’s archive.

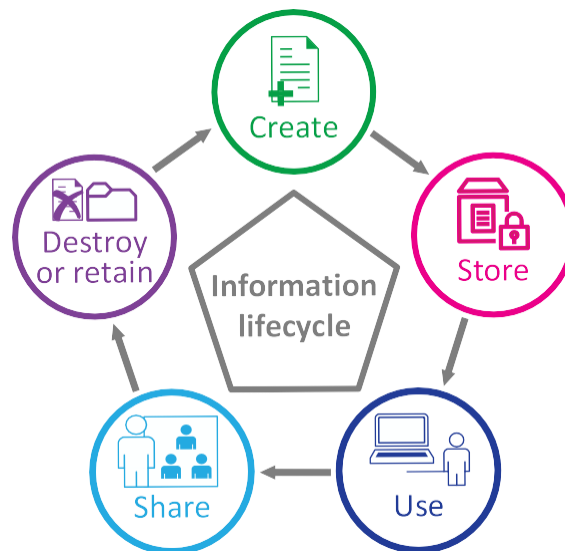


Figure 1: Information lifecycle

## 7. Capture and control of records

The Council uses a variety of systems to manage its records. These systems, regardless of the format of the records, must be designed to ensure that records are saved, stored, organised and managed effectively and efficiently.

The Council is committed to using appropriate systems to manage its structured records e.g. line of business systems or corporate records stores. Unstructured, electronic records will primarily be stored within M365 and managed with records management software (Avepoint Opus). This supports appropriate information sharing, aids search and retrieval processes and reduces the unnecessary duplication of records.

The corporate file plan and Records Retention Schedule will be applied to records when they are stored, created, or documented in M365. All documents and folders should be given names and metadata that facilitate meaningful use according to the Council's [Naming Standards](#).

## 8. Storage of records

Staff are encouraged to save in **electronic format** where appropriate for reasons of improved security, functionality and efficiency. Records should be stored on media that ensures that they can be retained and are accessible for as long as they are required, which in some cases is in perpetuity. **Paper records** held locally in offices should be locked away securely when not in use.

The Council has adopted the use of **M365**, particularly **MS Teams** and **MS SharePoint** for storing unstructured records. All Teams and SharePoint sites are allocated a function in the Council's file plan and staff should use the allocated sites for these records. Using unofficial storage areas, such as OneDrive, for records that should be managed under the file plan and Records Retention Schedule, will undermine efforts to effectively manage this corporate asset and puts the Council at risk of non-compliance with relevant legislation.

The Council operates a **records management service** for semi-current and non-current physical records, allowing services to store and access records off-site when they are not required for business use on a daily or weekly basis. This service manages intake of records, storage, destructions and transfers to archive, in line with the corporate Records Retention Schedule.

Service managers should ensure that they have a **contingency or business continuity plan** to provide protection for records which are vital to the continued functioning of the Council, in the event of a system outage or records being inaccessible because of e.g. fire or flood. The requirements are outlined in more detail in the [Vital Records Guidance](#).

## 9. Access to records

Appropriate procedures and processes should be put in place to ensure the physical, electronic and intellectual security of Council records. This facilitates the Council's ability to respond to requests for information under, for example, data protection and freedom of information legislation.

Access to information is governed by the statutory and regulatory framework within which the Council operates, and the business needs and requirements of the Council. Staff must comply with the relevant information policies, processes and procedures to protect records from unauthorised access.

## 10. Audit trail

An audit trail allows records to be tracked effectively, deters unauthorised access and can provide a method of monitoring changes to a document.

- The Council has demonstrated its commitment to tracking and monitoring records by migrating its unstructured records away from on-premises, network drives onto M365 which track all interactions with records automatically.
- Physical records held in two corporate records management stores, and the archives repository are tracked using Avepoint Opus.

## 11. Retention and disposal

There are substantial financial, legislative, and reputational risks associated with keeping records for too short or too long a time period. Retaining records for the correct period ensures compliance with a range of legislative requirements and promotes efficient information management. This is of particular significance for records containing personal data.

A corporate **Records Retention Schedule** enables staff to make informed decisions about retention and disposal of records across the Council and its partner organisations. The Records Retention Schedule is maintained and updated regularly by the Corporate Records Manager and the most up-to-date version is on the Council's website.

At the end of a record's disposal period, the **disposal actions** will be to:

- destroy,
- review for business value, or
- transfer to the archive.

The **Records Retention Schedule only applies to master records**. Duplicate, local or convenience copies should be destroyed as soon as they are no longer required. Short-lived documents such as telephone messages, meeting notes etc. should be transferred to a more formal document and saved as a record if they contain business critical information.

The Council acknowledges that there will be occasions when records cannot be destroyed in-line with the Records Retention Schedule because of legal proceedings or information requests.

## 12. Transfer to archive

North Lanarkshire Archives exists to collect, preserve and make available to the public the historical records of North Lanarkshire Council and its predecessor administrations. Its role is to maintain a traceable and uninterrupted line of care, control and possession of the Council's records from creation to preservation that serves as a means of protecting the authenticity of the records.

Arrangements for transfer of records to [North Lanarkshire Archives](#) are governed by the Records Retention Schedule and can take place on a regular basis or as one-off transfers. At the disposal date, the archivist should be contacted regarding records identified in the Records Retention Schedule as for permanent preservation, as being of historical value or to be offered to the archivist.

In some cases, only a sample of the records will be selected for permanent preservation, and the archivist will work with the service to select the most appropriate sampling method.

North Lanarkshire Archives has achieved Accredited Archive Status with the UK's Archive Service Accreditation Standard and has developed a suite of [procedures and guidance documents](#) concerning all aspects of collections and stakeholder management, in line with this standard.

Currently only physical records are being transferred to North Lanarkshire Archives however, in future, appropriate measures will be put in place to preserve digital records identified for permanent preservation as outlined in the [Digital Preservation Framework](#).

## 13. Destructions

**Electronic records** that are due for destruction should be deleted from Council systems. Records that are held on NLC servers are backed up for 5 weeks whereas records that are held on M365 will be backed up for a further 6 months before they become irretrievable.

**Physical records** that contain Council information should be securely destroyed by the Council's preferred third-party provider or shredded so that they cannot be reproduced.

## 14. Responsibilities

1. The **SIRO** is responsible for ensuring that all Council records are managed according to this policy.
2. The **Corporate Records Manager** is responsible for maintaining the Council's [Records Management Plan](#), providing procedures, advice and guidance on good records management practice, and ensuring that all service areas are supported by a Records Retention Schedule and file plans.
3. The **archives** are the designated place of deposit for Council records of continuing evidential and historical value, and the archivist is responsible for identifying, preserving, promoting and making accessible these records and other historical records that may be acquired by the Council.
4. All **managers** have day to day responsibility for records management and should ensure that systems are in place to enable compliance and that staff are familiar with and adhere to this policy and any related procedures, standards and guidance.
5. All **members of staff** must complete an introductory online training course in records management and are accountable to their supervisors for documenting their actions and decisions and for maintaining records and information systems in accordance with this policy and any related procedures, standards and guidance.

## 15. Product set

The table below lists documents in the Records and Information Management 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 Records and Archives team.
- Those listed under related products are the responsibility of other teams, services or agencies.

Product type	Product
Policies and plans	<ul style="list-style-type: none"> <li>▪ <a href="#">Records Management Plan</a></li> </ul>
Standards	<ul style="list-style-type: none"> <li>▪ <a href="#">Records Retention Schedule</a></li> </ul>
Guidance	<ul style="list-style-type: none"> <li>▪ <a href="#">Naming Convention Guidance</a></li> <li>▪ <a href="#">Archives Guidance</a></li> <li>▪ <a href="#">Digital Preservation Framework</a></li> <li>▪ <a href="#">Records and Information Management Guidance</a></li> <li>▪ <a href="#">Vital Records Guidance</a></li> <li>▪ <a href="#">Physical Records Management Guidance</a> <a href="https://nlc.gov.sharepoint.com/sites/InsideNL/SharedDocuments/Forms/AllItems.aspx?id=/sites/InsideNL/SharedDocuments/Information%20governance/Records%20and%20information%20management/Records%20Guidelines/Vital%20Records&amp;viewid=d26b8c9d-23ee-4fd7-9bb8-0d8ffb1815fe">https://nlc.gov.sharepoint.com/sites/InsideNL/SharedDocuments/Forms/AllItems.aspx?id=/sites/InsideNL/SharedDocuments/Information governance/Records and information management/Records Guidelines/Vital Records&amp;viewid=d26b8c9d-23ee-4fd7-9bb8-0d8ffb1815fe</a></li> </ul>
Related products	<ul style="list-style-type: none"> <li>▪ <a href="#">Data Protection Policy</a></li> <li>▪ <a href="#">Digital and IT Strategy</a></li> <li>▪ <a href="#">Information Asset Register</a></li> <li>▪ <a href="#">Information and Cyber Security Policy</a></li> <li>▪ <a href="#">Payment Card Data Security Policy</a></li> </ul>
Legislation, regulations, and government guidance	<ul style="list-style-type: none"> <li>▪ <a href="#">Archive Service Accreditation Standard</a></li> <li>▪ <a href="#">BS 15489-1:2016 Information and Documentation - Records Management</a></li> <li>▪ <a href="#">BS 4971:2017 Conservation and Care of Archive and Library Collections</a></li> <li>▪ <a href="#">Copyright, Designs and Patents Act 1988</a></li> <li>▪ <a href="#">Data Protection Act 2018</a></li> <li>▪ <a href="#">Freedom of Information (Scotland) Act 2002</a></li> <li>▪ <a href="#">Model Records Management Plan - National Records of Scotland</a></li> <li>▪ <a href="#">M365 Guidance</a></li> <li>▪ <a href="#">Public Records (Scotland) Act 2011</a></li> <li>▪ <a href="#">Re-use of Public Sector Information Regulations 2015</a></li> </ul>

Product type	Product
	<ul style="list-style-type: none"> <li>▪ <a href="#">Section 61 Code of Practice on Records Management under the Freedom of Information (Scotland) Act 2002</a></li> <li>▪ <a href="#">Scottish Council on Archives Record Retention Schedules (SCARRS) - Scottish Council on Archives</a></li> <li>▪ <a href="#">Supplementary Guidance on Proper Arrangements for Archiving Public Records</a></li> <li>▪ <a href="#">UK General Data Protection Regulation</a></li> </ul>

## Appendix 1: Glossary of terms

Term	Description
<b>Access</b>	The right, opportunity or means of finding, using or approaching documents and/or information in any format. Access may also be affected by the legal requirements and the physical condition of the materials, or the need to conserve them.
<b>Authenticity</b>	The trustworthiness of a record, i.e. the quality of a record that it is what it purports to be and that is free from tampering or corruption.
<b>The Council</b>	North Lanarkshire Council and North Lanarkshire Licensing Board.
<b>Disposal</b>	Action taken at the end of the retention period. This can be a decision to retain longer, transfer to the archive or secure destruction.
<b>File plan</b>	A file plan is a form of classification that arranges records by function. The M365 file plan arranges MS Teams and Sharepoint sites within functional hubs that mirror functions and activities as set out in the Records Retention Schedule.
<b>Information</b>	Data that has been given value through analysis, interpretation, or compilation in a meaningful form.
<b>Lifecycle</b>	The life span of a record from its creation or receipt to its final disposal.
<b>Non-current records</b>	Records no longer required for the work of the Council but retained for evidential purposes.

Term	Description
<b>North Lanarkshire Archives</b>	Contains records of any age and any format which are identified by the archivist as having long-term historical, evidential, or legal value. Exists to maintain a traceable and uninterrupted line of care, control and possession of the Council's records from creation to preservation that serves as a means of protecting the authenticity of the record.
<b>Records</b>	Information recorded, in any format or media, created, received, and maintained by the Council in the transaction of business, or the conduct of affairs and kept as evidence of such activity.
<b>Records Retention Schedule</b>	A comprehensive list of records series, indicating for each the length of time it is to be maintained after reaching a trigger date, and its method of disposition.
<b>Semi-current records</b>	Records that are still referred to on occasion for business purposes on an irregular basis.
<b>SIRO</b>	Senior Information Risk Owner - role held by the Chief Officer of Legal and Democratic with senior management responsibility for records management and information risk within the Council.
<b>Structured records</b>	Electronic information created or obtained by end users where the information is stored in tables in a relational database system such as line of business systems.
<b>Unstructured records</b>	Electronic information such as emails, word processing documents, spreadsheets, presentations and graphics – documents mostly created by individual users from desktop applications that are not relational databases. Unstructured records would also include Adobe PDF files and electronic captures of facsimiles as well as other image files.