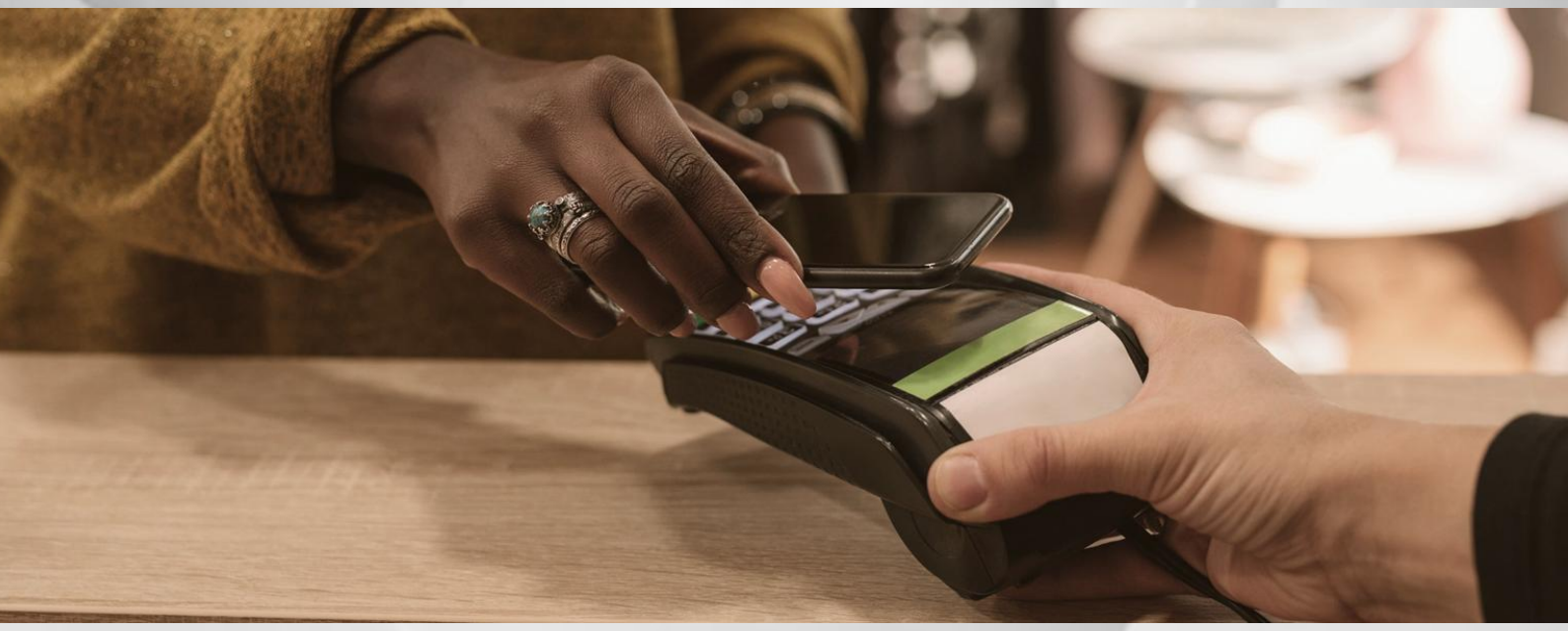
NORTH LANARKSHIRE COUNCIL
COMHAIRLE SIORRACHD LANNRAIG A TUATH

PAYMENT CARD DATA SECURITY POLICY

VERSION 2.01, MARCH 2026



LIVE
LEARN
WORK
INVEST
VISIT

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

Revision History

Number	Originator	Date review commenced	Revision description/record of change
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.

Document Approvals

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	

Consultation Record (for most recent update)

Status of document consulted upon	Stakeholders consulted between 11 March 2025 and 22 December 2025.	
Stakeholders consulted and dates	Data Management Team Technology Strategy Manager Data Governance Board PCI DSS Governance Board Corporate Management Team	11 March 2025 11 March 2025 26 March 2025 03 April 2025 22 December 2025

Strategic Alignment

Plan for North Lanarkshire

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

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 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.

Next review date

Review date	March 2028

Contents

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 – processes 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

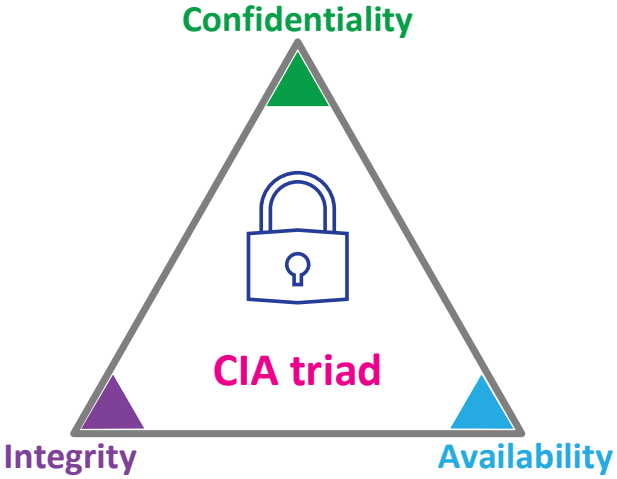
Only those who should see it, do see it.

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 (Legal, Democratic and Strategy)** – as the Council's Senior Information Risk Owner – is **accountable** for its governance.

The **Information Risk and Assurance team** is **responsible** for the following activities.

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

b. Report to management teams, governance and working groups, committees, and scrutiny panels.

5 Policy compliance

Every person 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. As per the note at the start of this policy, there are no active hyperlinks to files and web services used exclusively by council staff and elected members.
- Those listed under legislation, regulations, and government guidance are the responsibility of other agencies.

Product type	Product
Strategies	▪ Digital and IT Strategy ▪ Risk Management Strategy
Policies	▪ Acceptable Use of IT Policy ▪ Data Protection Policy ▪ Discipline Policy ▪ Information and Cyber Security Policy ▪ Records and Information Management Policy
Frameworks	▪ Security Standards Framework
Standards	▪ Information Classification and Handling Security Standard

Product type	Product
Procedures	▪ Code of Connection procedures ▪ Data Protection Breach and Incident Management Protocol ▪ Information Security Incident Management Procedure
Related products	▪ Records retention schedule ▪ Corporate procurement intranet document library ▪ LearnNL
Legislation, regulations, and government guidance	▪ Computer Misuse Act 1990: GOV.UK ▪ Copyright, Designs and Patents Act 1988: GOV.UK ▪ Cyber Resilient Scotland: strategic framework – Public Sector Action Plan: GOV.SCOT ▪ Data Protection Act 2018: GOV.UK ▪ General Data Protection Regulations ▪ Government Security Classification Policy: GOV.UK ▪ Government Security Classifications: GOV.UK ▪ Payment Card Industry Data Security Standard: PCI ▪ Payment Card Industry Security Standards Council: PCI ▪ Public Bodies (Joint Working) (Scotland) Act 2014: GOV.UK ▪ Public Records (Scotland) Act 2011: GOV.UK ▪ Public Services Network Connection Compliance: GOV.UK ▪ Strong encryption: PCI

Appendix A: Payment card data handling roles and responsibilities

Role	Responsibilities
Chief Executive of North Lanarkshire Council.	▪ Overall accountability for the protection of information the Council owns and processes.
Chief Officer of Finance and Technology The Council's subject matter expert on financial systems and solutions.	▪ 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. ▪ Accountable for putting in place policy, standards, and guidance in relation to financial solutions.
Senior Information Risk Owner (SIRO) The Chief Officer (Legal and, Democratic and Strategy) has this role.	▪ Make sure the Council protects both its information, and its information storage facilities and processing systems. ▪ Accountable for information and cyber security governance.
Corporate Management Team Members are the Chief Executive, Depute Chief Executive, SIRO, and Chief Officers.	▪ Sign off on information and cyber security controls and practices. ▪ Consider reports on the effectiveness of information and cyber security practices.
PCI DSS Governance Board A senior officer group with ongoing responsibility for PCI DSS.	▪ Provide executive management oversight of Council activities to make sure the Council complies with PCI DSS.
Data Governance Board A senior officer group of business information owners and subject matter experts from all services. Chaired by the SIRO.	▪ Assure robust information governance of this policy. ▪ Consider revisions before passing to the Policy and Strategy Committee for approval.

Role	Responsibilities

Data Management and Compliance Group
An officer group from all services with responsibility for business information including processes and IT systems.
	▪ Individual members must make sure their service complies with this policy and related standards, procedures and guidance.
	▪ Collectively the team:
	  ▪ oversees the review of this policy; and
	  ▪ agrees revisions before passing to the Data Governance Board to consider.

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

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

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

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

Everyone
As per the scope, every person who processes card payments and or handles cardholder data on behalf of the Council.
	▪ Follow policies, standards, procedures and guidance, and process card payments and protect cardholder data in line with them.
	▪ Keep up to date with:
	  ▪ mandatory training; and
	  ▪ general awareness communications.