Payment Card Data Security Policy

Version 1.0, 03 May 2023

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

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

Document control

Title	Payment Card Data Security Policy		
Governance group	PCI DSS Governance Board		
Owner	Katrina Hassell, Senior Information Risk Officer	**Contact**	hassellk@northlan.gov.uk
Author	Gordon Livingstone, Information Security Officer	**Contact**	livingstoneg@northlan.gov.uk

Revision history

Version	Originator	Review start date	Revision description and record of change
1.0	Gordon Livingstone	n/a	New policy.

Document approvals

Version	Governance group	Date approved	Date approval to be requested (if document still in draft)
4.0	Policy and Strategy Committee		08 June 2023

Consultation record (for most recent update)

Consultation status	Stakeholders consulted between October 2022 and April 2023.	
Stakeholders consulted and dates	Data Governance Board Data Management Team PCI DSS Governance Board	February 2023 March 2023 October 2022

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 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	

Contents

A note about plain English

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

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

1 Introduction

We take credit and debit card payments for a range of goods and services we provide – such as theatre tickets, special uplifts, council tax and housing rents. We must take card payments in a way that protects us and our customers from data breaches and fraud.

We use the following three **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; customers speak to our agents over the phone to make payments.

The Payment Card Industry Security Standards Council manages the Payment Card Industry Data Security Standard (PCI-DSS). This is a mandatory information security standard that applies worldwide, to every organisation that stores, processes, or transmits cardholder data. It helps us:

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

PCI-DSS is mandatory. Failure to comply with it could result in North Lanarkshire Council being fined and no longer permitted to process card payments.

---

2 Purpose

This Payment Card Data Security Policy sets out the controls we must use to protect the security of all card payments we receive and process. It makes sure we handle all card information securely and comply with all PCI-DSS requirements. It's also a control factor for the Information Security and Governance corporate risk and aligns with the following.

- Digital and IT Strategy – this brings together separate but related plans and policies – including this one – that contribute to our digital vision.
- Its sister policies – Data Protection, Information Security and Records and Information Management – that maintain the safety, confidentiality, integrity and availability of our information.
- Acceptable Use of IT Policy – this informs the council's IT users on how to appropriately use IT assets to store and process information.
- The Information Classification and Handling Standard – this controls how we classify and handle council information while safeguarding its confidentiality, integrity and availability.

3 Scope

This policy applies to all users of council IT assets who process, view or otherwise handle payment card data and cardholder details. This includes employees, councillors, contractors, consultants, temporary agency staff, modern apprentices, students, volunteers, and any other authorised third parties.

4 Governance

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

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

5 Policy compliance

Every person 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:

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

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

- Chief Executive
- Chief Officer of Financial Solutions
- Senior Information Risk Owner
- Corporate Management Team
- PCI DSS Governance Board
- Data Governance Board
- Data Management Team
- Information Risk Manager
- All managers
- Everyone in the scope of this policy with a duty for handling cardholder information.

6 Policy objectives

This policy sets our 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 we use to store, process and transmit it.
2. Help everyone who processes card payments and or handles cardholder data understand:
   a. why we must protect its confidentiality, integrity, and availability;
   b. the controls we use to protect it; and
   c. their role in this.
3. Show our key stakeholders – such as elected members, residents, customers and service users – that we treat and protect cardholder data in line with its value and sensitivity.
4. Provide a development and review process for payment card data security standards, procedures, and guidance.

7 Payment card data security controls

7.1 Information security

The Information Security Policy sets out a range of controls to protect and manage our information. They all apply to payment card data and include:

- managing risk;
- managing information;
- training and awareness; and
- operational security.

7.2 Information classification

The Information Classification and Handling Standard outlines how we classify and mark information assets and lists our information handling rules. The Information Classification and Handling Guidance details how we apply the standard.

We always classify and handle cardholder details as OFFICIAL-SENSITIVE – PERSONAL.

7.3 Access to cardholder data

We control access to cardholder data in line with the Access Control Standard and the Records and Information Management Policy. We must also apply the following payment card data access controls.

- Clearly define job functions that must access cardholder data.
- Restrict and pre-authorise all access to cardholder data.
- 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**).
- Restrict access to all 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.

7.4 Third-party service providers

We use third-party service providers to process card payments, subject to the following mandatory controls.

- Use our established corporate procurement processes, including formal due diligence, before engaging with a service provider.
- All contracts with third-party service providers must include a specific agreement that the service provider is responsible for the cardholder data they hold; and
- All third-party service providers are contractually obliged to comply with PCI-DSS
- Formally monitor the service provider's PCI DSS compliance status.
- Keep a list of all third-party service providers we share cardholder data with.

7.5 Physical security

We must prevent unauthorised individuals from accessing sensitive data. To do this we physically restrict access to sensitive information assets in both digital and paper formats.

Information assets

Digital

→ Hosted within our own network and on cloud-based services.

→ May also be stored on devices such as laptops, phones, tablets, and other external storage media such as USB flash drives and memory cards.

→ Includes computer files such as documents, spreadsheets, records in business systems.

Paper

→ Stored in council facilities and any third-party locations.

→ Includes printed or handwritten documents, received faxes.

The Information Classification and Handling Guidance details all handling rules. We must also apply the following controls for payment card data and machines.

- Only those authorised to do so can handle and distribute information assets that contain sensitive data. They must do this in a secure manner.
- Trusted employees must escort visitors at all times when in areas that hold sensitive cardholder information.
- Keep a list of all payment card machines that:
  - → includes the make, model, location, serial number or other unique identifier; and
  - → we update whenever we add, remove or relocate a machine; and
- Routinely check payment card machine surfaces to detect if they've been tampered with or swapped out with an unauthorised machine for fraudulent purposes.
- Everyone who uses payment card machines must receive training on how to:
  - → use payment card machines;
  - → properly handle cardholder details; and
  - → identify and report suspicious behaviour and possible tampering.
- Always check and verify the identity of anyone claiming to be from an authorised third-party personnel who wants to install, replace, repair or run maintenance tasks on, or otherwise access our payment card machines.

7.6 Protect stored data

The Information Classification and Handling Guidance details storage rules. We must also protect cardholder data using the following controls.

- Always protect cardholder data against any unauthorised use.
- Securely destroy any sensitive card data that we no longer need so that its unrecoverable – in line with the Records retention schedule.
- Don't display full long card numbers. Don't display the full number onscreen – as detailed in access to cardholder data above – unless there's a need to show it all.
- **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.

7.7 Protect data in transit

We must use the following controls to protect cardholder data when transmitting it digitally or transporting it physically.

- Never send any card details – full long card number, track data, security code, PIN, PIN block – across or outside our network using messaging services such as email and chat, or any other unencrypted or unauthorised system or service.
- If there is a business reason to transmit or transport cardholder data, the appropriate manager must authorise it first and we must use the following safety controls.

→ Digitally – using email or another digital system or service – use a strong encryption mechanism.
→ Physically – log and inventory the data before leaving the premises. Only use secure courier services. Monitor the shipment status until it you receive delivery confirmation.

7.8 Disposal of stored data

As detailed in the Information Classification and Handling Guidance we must do the following.

- Securely delete all digital data – on all systems and services – when we no longer need it.
- Destroy all hard copies of cardholder data when we no longer have a valid business reason to keep it.
- Use lockable storage containers – clearly marked for secure and sensitive disposal – to store all cardholder data awaiting destruction. Restrict access to these containers.

7.9 Training and awareness

The Information Security Policy details how we use training and awareness to help manage information risk. This includes:

- **Mandatory training modules** on LearnNL covering the core elements of information governance.
  → Data protection
  → Information security
  → Records and Information management
- **Awareness raising activities** to promote information security, share information and build knowledge.

We also provide specific training for using payment card processing systems and services.

7.10 Information security incidents and data breaches

The Information Security Incident Management Procedure and the Data Protection Breach and Incident Management Protocol explain how we react to actual and suspected security incidents and data breaches. The Cardholder Data Breach Incident Response Plan details how we handle incidents involving cardholder data breaches.

8 Product set

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

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

Product type	Product
Policies	▪ Acceptable Use of IT Policy ▪ Information Security Policy

Product type	Product
Standards	▪ Access Control Standard ▪ Information Classification and Handling Standard
Procedures	▪ Information Security Incident Management Procedure
Guidance	▪ Information Classification and Handling Guidance
Related products	▪ Cardholder Data Breach Incident Response Plan ▪ Corporate procurement document library on InsideNL ▪ Data Protection Breach and Incident Management Protocol ▪ Data Protection Policy ▪ Digital and IT Strategy ▪ Information Asset Register ▪ LearnNL ▪ PCI Security Standards Council ▪ Records and Information Management Policy ▪ Records retention schedule ▪ Strong encryption

Appendix 1: Payment card data handling roles and responsibilities

Role	Responsibilities
Chief Executive of North Lanarkshire Council.	▪ Overall accountability for the protection of information we own and process.
Chief Officer of Financial Solutions The council's subject matter expert on financial systems and solutions.	▪ Overall accountability for protecting financial data and making sure financial systems and processes comply with PCI DSS. ▪ Accountable for putting in place policy, standards, and guidance in relation to financial solutions.

Senior Information Risk Owner (SIRO)
The Chief Officer of Business and Digital has this role.
	▪ Make sure we protect our:
	  ▪ information; and
	  ▪ information storage facilities and processing systems.
	  ▪ Accountable for information security governance.

Corporate Management Team The council's executive board. Members are the Chief Executive, Depute Chief Executive, SIRO, and Chief Officers.	▪ Sign off on our information security controls and practices. ▪ Consider reports on the effectiveness of our information security practices.
PCI DSS Governance Board A senior officer group with ongoing responsibility for PCI DSS.	▪ Provide executive management oversight of council activities to make sure we comply 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.

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

Role	Responsibilities

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

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

Everyone
As per the scope, every person who processes card payments and or handles cardholder data.
	▪ 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.