Policy name	Card Payment Security Policy
Subject	Secure card payment processing
Approving authority	Assurance Committee
Accountable person	Chief Financial Officer
Responsible Team	Financial Control
First approved	June 2024
Last updated	June 2024
Version number	V1

1 Introductory Purpose and Background

The Payment Card Industry Data Security Standard (PCI-DSS) is a set of global security standards set by the PCI Security Standards Council that organisations must follow to protect sensitive payment card information from theft and fraud.

As the University processes and transmits payment card data, we are required to comply with PCI-DSS to protect our students, staff, and customers' payment card information. The University takes its responsibility to protect payment card information seriously. This policy outlines the steps we are taking to comply with PCI-DSS requirements and protect our students, staff, and customers' payment card information.

2 Scope

This policy applies to all faculties, schools, departments, systems, and individuals or third parties involved in processing and transmitting payment card for the University of Nottingham UK.

3 Definitions

Payment Card Industry Data Security Standard (PCI-DSS) - The global set of security standards established by the PCI Security Standards Council that organisations must follow to protect payment card data.

Cardholder Data - Any data related to a payment card, including account number, expiration date, CVV code, etc.

Encryption - Encoding data to prevent unauthorised access during transmission and storage.

E-Commerce - Online business activities such as sales through websites and mobile apps.

Firewalls - Network security systems that control incoming and outgoing network traffic.

Multi-Factor Authentication - Authentication method that requires two or more verification factors, like a password and a one-time code.

PCI Compliance Assessment - Annual audit to verify compliance with PCI-DSS requirements.

Data Breach - Security incident involving unauthorised access to sensitive cardholder data.

Business Units - Schools, departments, and other units of the University that process payment card transactions.

Heads of Schools and Heads of Professional Services - Leadership roles such as deans, directors, department heads.

Chief Financial Officer (CFO) - Senior executive responsible for the University's finances.

Chief Information Security Officer (CISO) - Senior executive responsible for the University's information security.

Financial Control Department - Department responsible for managing PCI compliance.

Individuals and third parties are:

- Customer facing staff accepting card payments either face to face, by phone and/or by mail.
- Staff maintaining systems connected to or involved with card payments processing.
- Payment service providers (PsPs).
- Payment Card acquirers.

Payment card acquirers - are banks or financial institutions that process payment card transactions on behalf of a merchant and pay the merchant the funds obtained from card transactions.

Payment Service Providers - are third parties who process, store and/or transmit card payment data for the merchant through to Payment Card acquirers, including service providers who host websites which redirect to a secure payment page.

4 Policy

Key roles, responsibilities and/or requirements

4.1 Key Principles

All Business units wishing to receive payments via payment cards must engage with the Financial Control Department to seek authority to proceed, and to ensure compliance with this policy.

4.2 Responsibilities

The Chief Financial Officer (CFO) is accountable for compliance with the Payment Card Industry Data Security Standard (PCI-DSS) within the University, and the management of risks related to non-compliance.

The Financial Control Department is responsible for managing PCI DSS compliance across the University and may remove any payment card processing activity causing unacceptable risk.

The Chief Information Security Officer is responsible for the management of risks related to the protection of payment card data and associated cyber threats.

Heads of Schools and Heads of Professional Services are responsible for ensuring that their staff required to take payment via cards have received the necessary training as set out within the Standard Operating Procedure supporting this policy.

Financial Control is responsible for establishing a PCI framework of standards and procedures to ensure ongoing compliance with the contractual requirements from our partner acquiring banks. Financial Control is responsible for ensuring regular checks of business units are conducted to ensure compliance with the universities PCI framework.

4.3.1 Data Security

i) Cardholder data should only be processed and transmitted if it is necessary for the University's business purposes.

ii) All payment card information should be protected with industry-standard encryption during transmission.

iii) Card data must never be stored on University systems, either digitally or on paper.

4.3.2 E-commerce

Business units intending to engage in ecommerce activities either through websites, applications or other software must seek approval from Financial Control prior to proceeding.

All payment solutions must either be:

i) provided by a third-party vendor whose solution appears on the list of validated applications published by PCI council.
ii) or developed in line with University website development policy and comply with the current PCI Secure Software Standard and will be subject to regular compliance scans.

4.3.3 Network Security

The University's network must be protected with a firewall and other security measures to prevent unauthorised access.

- Access to the network must be restricted to authorised personnel only.
- All wireless networks must be secured with encryption and have a strong password.
- Remote access to the University's network must be protected with multi-factor authentication.

4.3.4 Physical Security

Payment card information should be processed and transmitted in a secure location that is accessible only to authorised personnel.

Access to areas where payment card information is processed and transmitted should be restricted to authorised personnel only.

4.4 Compliance

i) The University must conduct an annual PCI-DSS compliance assessment.
ii) The University must comply with all PCI-DSS requirements and take appropriate steps to remediate any issues identified during the assessment.
iii) The University must maintain appropriate documentation to demonstrate compliance.

Incident Response

i) The University must have a documented incident response plan that outlines the steps to be taken in the event of a data breach or other security incident. The plan must be visible to the CISO and the Financial Control Department.
ii) All incidents must be reported to the appropriate personnel immediately.
iii) The University must work with the appropriate authorities to investigate the incident and take appropriate steps to remediate any damage caused.

Training and Awareness

i) All personnel involved in the processing and transmission of payment card information must receive appropriate training and awareness.
ii) All personnel must be aware of the University's PCI-DSS policy and their responsibilities under this policy.
iii) The University must conduct regular training and awareness sessions to ensure all personnel are up to date with the latest security best practices.

Failure to comply with this policy could result in the removal of the terminal/ payment option for the non-compliant area and disciplinary action, up to and including termination of employment.

Failure to comply with the standards, or a breach of payment card data would result in significant reputational damage for the University as the PCI Security Standards Council and the UK Information Commissioner may apply financial sanctions.

Non-compliance could also result in the removal of the University's ability to receive card payments.

4.5 How compliance with the policy will be measured.

Adherence to policy will be measured by random audits of terminals and training by Financial Control on Business Units taking card payments.

4.6 Provisions for monitoring and reporting related to the policy.

Audit results and any issues identified will be discussed by the University's PCI Governance group and any potential breaches will be investigated and escalated to the Assurance Committee.

5 Review

This policy is reviewed and updated annually.

6 Related policies, procedures, standards, and guidance

Information Security Policy
Data Protection Policy
Data Handling Policy (internal access only)
Personal Data Breach Procedure