UNIVERSITY OF ABERDEEN

PAYMENT CARD SECURITY POLICY

1. Background

1.1. This policy supports the University of Aberdeen achieving and maintaining Payment Card Industry Data Security Standard (PCI DSS) compliance. PCI DSS is the minimum level of card data security set by the Payment Card Industry Security Standards Council. It aims to reduce the risk of theft and fraud of sensitive cardholder data by ensuring a safe and secure environment for customer card data to be received, used, transmitted or stored.

1.2. PCI DSS is a mandatory requirement. Failure to comply with the standard will, in the event of a card security breach, result in higher fines and increased transaction charges. Failure to comply may result in the University of Aberdeen being denied permission to accept card payments in the future, as well as further investigation by other regulatory bodies such as the Scottish Charity Regulator (OSCR) and the Information Commissioner's Office (ICO).

1.3. The University accepts card payments for goods and services, donations on campus, and payment of debt. Card payments are accepted by a variety of methods including online, in person, and through third party providers. The University transmits card holder data on its IT networks for both its own and for third party sales.

1.4. Adherence to this policy will assist in reducing the risk and impact of a data breach, including subsequent fines and charges, and ensures adequate safeguards are in place to protect sensitive cardholder data. Failure to comply with this policy may result in disciplinary action.

2. Responsibilities

2.1. The requirements of PCI-DSS compliance involves significant input and co-operation between both the Directorates of Finance and Digital and Information Services.

2.2. The Chief Financial Officer is responsible for ensuring the University of Aberdeen's overall PCI-DSS compliance.

2.3. The Director of Digital and Information Services is responsible for providing a secure network environment which adheres to payment card security standards and its associated requirements and the provision of a qualified Internal Security Assessor (ISA).

2.4. Schools and Directorates with card payment devices are responsible for adhering to all policies relating to payment card acceptance including nominating a point of contact for queries or issues, advising Finance of all movements in devices, ensuring all staff with access to cardholder data or devices undertake the mandatory annual Payment Security Training.

2.5. Third party service providers, and third-party vendors transmitting cardholder data on the University networks, must be PCI DSS compliant and are responsible for maintaining their own compliance. They must provide evidence of compliance on request.

2.6. The Data Protection Officer (DPO) has statutory remit to monitor the University's compliance with the UK General Data Protection Regulation and the Data Protection Act 2018, which would include personal data processed as part of the payment activities.

2.7. The Information Governance Committee has executive responsibility for information governance compliance and information security assurance within the University, and for taking steps to address risks and areas of concern.

2.8. The Information Risk Working Group is responsible for reviewing information governance and security risk and advising on risk treatment efforts and consistent implementation of this Policy.

2.9. The Internal Security Assessor (ISA) will recommend and advise on PCI DSS security standards for implementing and maintaining card payment methods to ensure compliance.

3. Accepting Card Payments

3.1. The need for payment card devices should be minimised by processing sales through the online store, EventsAir platform, or by issuing a sales invoice where possible. Where there is a genuine business need to accept card payments in person, the School/Directorate must submit a request to the Treasury Manager, Finance, and if approved, Finance will work with the requesting area to identify a suitable payment solution.

3.2. New card payment methods or changes to existing card payment methods must be requested through and approved by the Treasury Team, Directorate of Finance.

3.3. Finance will maintain a register of all card payment methods and devices.

3.4. All Schools/Directorates accepting card payments in any format, must adhere to all policies and procedures detailed in this and any other supporting documentation, failure to do so may result in the removal of the payment device and the area being unable to accept card payments.

3.5. Payment methods that are implemented without obtaining the appropriate permissions and/or do not meet the required standards will be removed from service.

4. Online Payments

4.1. All online payment acceptance methods must be requested through, and approved by the Treasury Team, Directorate of Finance. This includes utilising third party providers of online sales services.

4.2. All third-party partners and payment service providers involved in the provision of online payment card services must evidence their PCI-DSS compliance when requested. Compliance must be requested and evidenced prior to the commencement of services, and on an annual basis for the duration of the service.

4.3. Finance is responsible for maintaining a list of online payment service providers and partners, and for ensuring their supporting compliance documentation is obtained on an annual basis.

4.4. Cardholder data accessed through online platforms must be obscured. This is to reduce the risk of theft of cardholder data and minimise the impact of the accompanying breach. All online payment transactions must use strong cryptography, including TLS 1.2 or higher, in accordance with PCI DSS v4.0. Encryption standards will be reviewed annually.

4.5. Only University staff with a genuine business need will be provided with a unique login to access online card payment data. Users must not share their log in details.

4.6. Third party online payment card platforms must only be accessed from secure University devices. Payment card sites must not be accessed through personal devices or publicly shared University devices.

5. Payment Card Devices

5.1. All payment card devices (virtual or physical) must be requested through and approved by the Treasury Team, Directorate of Finance.

5.2. Finance will maintain a register of all devices including location, unique device identification numbers, model type and key contacts.

5.3. All third-party partners and payment service providers involved in the provision of payment card services using these devices, must evidence their PCI DSS compliance when requested. Compliance must be requested and evidenced prior to the commencement of services, and on an annual basis for the duration of the services.

5.4. Finance is responsible for ensuring compliance documentation is obtained from all partners and payment service providers on an annual basis.

5.5. The payment card environment will be segregated/segmented from other networks where possible. Only traffic that is necessary is allowed into the payment card network and all other traffic specifically denied.

5.6. All payment card devices must use end-to-end encryption or PCI-validated Point-to-Point Encryption (P2PE) solutions where available. This includes third parties using University networks to transmit cardholder data.

5.7. Payment card devices must not be added to the University's network without prior consultation and authorisation from the Treasury Manager, Finance, and Digital and Information Services. This includes devices using WIFI, blue tooth, GPRS, or any other transmission method.

5.8. Schools/Directorates will be notified in advance by Finance if device software or hardware updates are required, and from Digital and Information Services if updates are required for network connections points. Without advance notification from the appropriate Directorate, no individual is permitted to update or change a device or its network connection. Updates will be pushed out automatically by the terminal provider where required.

6. Payment Card Device Security

6.1. Physical card devices (also known as PIN Entry Devices, PEDS or card terminals) must be located in a secure environment.

6.2. Devices which are unattended must be appropriately secured e.g. secure cradle, under CCTV coverage, with regular checks being performed.

6.3. Any movement in location or network port connection of a device must be notified to Finance in advance of the change. Finance will update the register of card payment devices.

6.4. Schools/Directorates may be requested by Finance to apply security updates to their devices, these updates must be applied immediately. There may also be updates pushed automatically to the devices by the terminal provider.

6.5. All devices must be inspected regularly, and as a minimum before the commencement of service. The purpose of inspecting devices is to identify signs of tampering at the earliest opportunity and so reduce the impact of fraud. Tampering may be in a physical form such as skimming devices or swapping of terminals, or a change in performance which may indicate the presence of malware.

6.6. Schools/Directorates are responsible for undertaking regular device inspections in accordance with the Card Payment Device Inspection Procedure.

6.7. An audit log of all device inspections must be maintained, and the log submitted to Finance monthly, or on request.

6.8. If a School/Directorate fails to inspect their payment devices and/or submit the audit log, their payment device may be removed from service.

6.9. All discrepancies must be investigated, and the device disconnected and removed from service until the situation is resolved. All incidents must be reported to Finance as detailed in the Card Payment Device Inspection Procedure.

6.10. Devices must be returned to Finance if no longer required or at the end of contract.

6.11. Finance will dispose of payment devices in a secure and appropriate manner i.e. as directed by the service provider.

7. Payment Device Supervisor Cards

7.1. Due to the additional access granted by a payment device supervisor card, access to the card and PINs must be strictly limited to those with a genuine business need and appropriate responsibility.

7.2. Supervisor cards must be kept secure and must not be stored with the payment device.

8. Cardholder Not Present Payments

8.1. Cardholder Not Present (CNP) payments include telephone payments and payments submitted in written format.

8.2. Schools/Directorates must never request customers to submit payment card details in written format including paper, email, text or any other electronic format. This includes requesting details to allow refunds to be processed.

8.3. If cardholder details are received electronically the details must not be forwarded (including replies to emails, etc). All sources of the data must be fully deleted immediately, and the customer contacted and advised not to submit payment card details in this format.

8.4. In the event that the University receives cardholder details in paper format, these must be destroyed by cross shedding and disposed of in secure confidential waste.

8.5. The following sensitive authentication cardholder data must never be stored in any format:

- The contents of the payment card magnetic stripe (track data)
- The CVV/CVC/CID – the 3 or 4 digit number on the signature panel on the reverse of the payment card
- The PIN or the encrypted PIN Block.

8.6. Telephone payments (including Microsoft Teams) must not be accepted on standard University connections. Telephone payments can be accepted if additional telephone network security is approved by IT and implemented in advance.

8.7. Customers should be requested to make payment by an appropriate alternative means, for example through the University's Online Store, EventsAir platform, or as detailed on the University's Making a Payment web pages.

8.8. Finance will request Cardholder Not Present payments are blocked on payment devices where possible

9. Payment Card Receipts

9.1. Receipts are set to obscure the Primary Authentication Number (PAN) as standard. This is to reduce the quantity of unnecessary cardholder data collected and requiring to be held securely.

9.2. All receipts must be treated as sensitive data and stored in a secure location. Only individuals with a genuine business need should be granted access to the receipts.

9.3. Receipts must be disposed of no later than 3 months after the date of sale.

9.4. All receipts must be disposed of in secure confidential waste.

9.5. Cardholder data must not be used for any other purpose than that intended i.e. payment acceptance and related refunds.

10. Refund Processing

10.1. For Anti Money Laundering purposes payment card refunds must, wherever possible, be processed to the original payment card.

10.2. Online Store refunds will be processed through the Online Store. EventsAir refunds will be processed though the EventsAir platform. In instances where a School or Directorate has a regular requirement to process refunds, access to this functionality may be granted, all other online store refunds will be processed by Finance.

10.3. Refunds of online payments of sales invoices will be processed by Finance using the payment service provider's portal.

10.4. Over the counter purchases processed on a physical payment device may be refunded by the School/Directorate to the original payment card.

10.5. Refunds of invoices where payment was processed on a physical payment device should be referred to Finance unless prior permission has been granted for the School/Directorate to process this type of transaction. To ensure the customer account is accurate and the audit trail complete, refunds of customer sales invoices must be processed and matched to a credit note in the Finance System.

10.6. In instances where the refund cannot be processed to the original payment card because the card has expired or the allowable refund period has passed (online payments), the customer will be contacted by Finance, and new refund details obtained.

10.7. The refund must be paid to the original payee. Finance will apply appropriate checks to verify the identity of the original payee and ensure the refund is returned to them.

11. Staff Training

11.1. All staff are responsible for adhering to the University of Aberdeen's policies relating to payment acceptance and security.

11.2. Staff with access to the cardholder data must undertake mandatory Payment Security Training within 1 month of starting their role and complete refresher training each year.

This includes:

- All staff who accept card payments, even if infrequently
- All staff located in the area where a payment card device is located
- All staff who support payment processing in any format e.g. process or store merchant copies of receipts on which full card numbers are displayed

11.3. Training will also include role-specific modules tailored to the staff member's responsibilities.

11.4. Finance is responsible for providing access to appropriate Payment Security Training for staff. Digital and Information Services will support in the content of training, particularly any role-specific training for Digital and Information Services staff.

11.5. Training will include, but is not limited to, understanding the importance of payment card data security, device security, and the incident response plan.

11.6. The School/Directorate is responsible for identifying and ensuring all relevant staff undertake the Payment Card Security Training within their area.

11.7. If a School/Directorate fails to ensure all relevant staff undertake the annual training, the payment device may be removed, and the area will not be permitted to accept card payments.

11.8. Staff who are unable to undertake the mandatory training due to long term absence e.g. maternity leave or sick leave, must undertake the training on their return to work and prior to accepting payment by card or accessing areas with cardholder data.

11.9. A roaming terminal is available for ad hoc events however PCI DSS training must be undertaken by all staff who will be using the terminal before it will be given out. Audit logs will be required, as well as a staff member signing the terminal out.

12. Incident Response

12.1. The Directorate of Finance will maintain and align the Payment Incident Response plans to the UoA Cyber Incident Response Plan.

12.2. In the event an incident is identified e.g. a payment device is suspected of being tampered with, the School/Directorate must remove the device from service immediately and unplug it from networks and/or systems then invoke the Cyber incident response plan

12.3. The nominated individual identified on the Payment Card Device Inspection Procedure should be contacted immediately. If the nominated individual and their delegated substitute are both absent the device must be removed from service and the incident reported to Finance immediately.

12.4. The nominated individual (or Finance) will investigate the matter, if satisfied the device has not been tampered with it can be returned to service. If there is any concern over the security or integrity of the device, it must not be returned to service.

12.5. All incidents must be logged and reported to Finance who will undertake further investigations if required.

12.6. Finance is responsible for reporting all incidents or breaches to the Information Security and Data Protection Officer. Where required to do so, the Data Protection Officer will report any personal data breaches to the Information Commissioner's Office in accordance with UK GDPR requirements.

12.7.

The Incident Response Plan will be tested at least annually through live simulations and/or tabletop exercises to validate compliance. This may include periodically performing unannounced checks of devices or logs.

13. Information Security

13.1. It is University of Aberdeen policy to maintain a level of payment security that meets or exceeds the requirements of the Payment Card Industry Data Security Standard (PCI DSS).

13.2. Payment security activities and controls will be subject to both internal and external audits as required for PCI DSS compliance.

13.3. Firewalls are required to control the transmission of data between the cardholder data environment, trusted internal networks and untrusted external networks.

13.4. Network devices and systems will have default passwords changed, security configuration assessed, and unnecessary default services and accounts removed prior to deployment.

13.5. Cardholder data storage will be kept to a minimum and be securely encrypted when in transit across a network and at rest. Strong cryptographic algorithms must be used, in line with current PCI DSS standards. Legacy protocols (e.g., TLS 1.0/1.1) are prohibited.

13.6. Where possible, all systems used within the cardholder data environment will be protected against malware with anti-virus software.

13.7. Internal vulnerability scans will be performed monthly. External vulnerability scans will be performed quarterly. Remediation activities will be performed in line with the University of Aberdeen vulnerability management procedure.

13.8. External vulnerability scans will be performed by an Approved Scanning Vendor (ASV) certified by the Payment Card Industry Security Standards Council (PCI SSC) in accordance with the standard's requirements.

13.9. Internal and external penetration tests will be carried out at least once a year.

13.10. Cardholder data will only be accessible to personnel who have a legitimate business reason because of a job or activity they are authorised to undertake.

13.11. Individuals who handle or have access to cardholder data will be identifiable and authenticated in compliance with the University of Aberdeen Authentication Policy.

13.12. Information security related logs will be kept for at least 1 year with a minimum of three months immediately available.

13.13. Cardholder data will be retained for the minimum time possible in line with business need and be destroyed immediately after usage, or when retention period has expired.

13.14. A cyber incident response procedure that is suitable for responding to potential incidents that may impact the confidentiality, integrity or availability of cardholder data will be maintained and tested at least annually.

14. Review

This policy is reviewed on at least an annual basis. Reviews will also take place whenever PCI DSS standards are updated, or when significant changes occur in relevant UK legislation to ensure it:

- Remains fit for purpose.
- Reflects changes in technologies and requirements.
- Is aligned to industry best practice.
- Supports continued regulatory, contractual, and legal compliance.

15. Supporting Policies, Procedures and Documentation

- Authentication Policy
- Information Security Policy
- Data Protection Policy
- Records Management Policy
- Cyber Incident Response Plan
- Card Payment Device Inspection Procedure
- Card Payment Device Inspection Log
- Payment Card Training

Document Control

Version	Date	Action
1.0	December 2021	Approved – Information Governance Committee Approved – Senior Management Team
2.0	December 2024	Approved – Information Governance Committee
3.0	December 2025	Approved – Information Governance Committee

Title	Payment Card Security Policy
Author / Creator	Lauren Johnston and Fiona Stuart
Owner	Finance with support from Digital and Information Services
Date published/approved	TBC
Version	3.0
Reviewed	October 2025
Date of next review	October 2026
Audience	All staff involved in the processing of credit/debit card payments and staff who support the processing of credit/debit card payments.