Payment Card Security Policy

Glasgow Caledonian University Payment Security

Status	Final
Owner	Treasury
Source location	Finance Website
Reviewed	March 2026
Next Review	March 2027
Version No	V001 06/2026

1. BACKGROUND

Glasgow Caledonian University accepts debit and credit card payments online, and in person (face to face). In person, payments are processed on physical payment devices at Three locations across the University (Vision Centre, Arc & Print Services). Wherever possible, the processing of card data should be undertaken by third party service providers who are licensed/accredited to process such data in line with the standard (WPM and Flywire).

The Payment Card Industry Data Security Standard (PCI DSS) is a worldwide information security standard defined and published by the Payment Card Industry Security Standards Council. The purpose of the standard is to reduce the risk of theft and fraud of sensitive cardholder data by providing a secure environment for customers to make payment. It applies to all organisations that receive, process, store and exchange cardholder information, whether digitally or manually. An organisation's merchant services provider on behalf of the major card brands will enforce compliance. For the University the merchant service provider is currently Global payments. Failure to meet the compliance requirements will result in increased transaction charges and the University could risk losing their ability to process card payments.

The University must demonstrate its compliance with the standard by completing an annual self-assessment questionnaire (SAQ), or more frequently if there is any change to the payment card environment, for example introducing new methods of card payment or changing devices.

This Payment Card Security Policy assists the University in complying with the legal requirements of the Standard. It will assist in reducing the risk and impact of a data breach, including subsequent fines and charges, and it ensures adequate safeguards are in place to protect sensitive cardholder data.

2. RESPONSIBILITIES

This policy is mandatory for all University staff. Failure to comply with this policy may result in disciplinary action.

Finance, supported by IT Services, is responsible for ensuring the University maintains PCI DSS compliance. Schools & Departments must not implement business processes that involve the processing of card payments without first consulting with Finance.

All staff at locations on campus, where card payment devices (physical or virtual) are held, are responsible for adhering to the following:

- all policies relating to payment card acceptance,
- Complete Updated Annual Training provided by IT,
- nominate a point of contact for queries or issues,
- advise Finance of all movements in devices

Finance will maintain a current list of all card payment methods and devices. Payment methods that are implemented without obtaining the appropriate permissions and/or do not meet the required standards will be removed from service.

In the event of there being a breach of data, staff must follow the University Incident Response Plan and immediately contact IT services.

3. PAYMENT CARD PROCESSING

Online Payment Processing

This is the University's preferred method for taking card payments, as the approved payment service provider is responsible for handling the cardholder data, not the University. The benefit of using payment service providers is that the University retains no card details processed through an approved online system. Wherever possible students, staff and customers should be directed towards the University's online payment services and online payment pathway facilities.

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, on an annual basis, by the University's Treasury representatives. Treasury as evidence of compliance will retain these certificates.

Customer Present Card Transaction

Where it is not possible to use online payment processing, the use of approved card processing terminals is permitted. These are currently located in the Vision Centre Print Services and Arc. Treasury maintains an inventory of all authorised PDQ machines that are used for card transactions.

All PDQ machines must have end-to-end encryption. This means that the payment data is transmitted to the payment service provider in an encrypted (unreadable) format. They are then able to decipher the transmission through their systems and process the payment. To reduce the risk of a data breach, PDQ machines capable of storing or transmitting unencrypted data must not be used.

Card payments can only be processed by one of these authorised devices. All PDQ machines should be connected the Roaming Sim Card (provided inside the PDQ machine) and should not be connected to any University system or network including Wi-Fi.

Card Details Received in Writing

The University, under no circumstances accepts card details in written format. If cardholder data is received, the details must not be forwarded and all sources of the data must be deleted immediately. The customer should then be contacted and advised not to submit payment card details in written format.

With the exception of merchant copies of receipts (full card data obscured) retained by the various locations, full cardholder data must not be stored or retained in any format including electronically or on paper. The following sensitive authentication cardholder data must never be stored in any format:

- The contents of the payment card magnetic strip (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.

4. PAYMENT CARD RECEIPTS

All receipts, regardless of whether the Primary Authentication Number (PAN) is displayed in full or not, must be treated as sensitive data and should be stored in a secured location. It is the responsibility at the various sites to ensure this happens. Only individuals with a genuine business need should be granted access to the receipts.

Receipts must be disposed of through confidential waste either in a restricted access confidential waste bin or dedicated pick up no later than one month after the date of sale. All confidential waste should be cross-shredded.

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

5. REFUND PROCESSING

For Anti-Money Laundering purposes, refunds must, where possible, be processed back to the original payment card.

A member of the finance team will process refunds through the online store and the payment service provider's portal.

Over the counter purchases can be refunded by the staff located on site where the PDQ device is held. The refund must be processed back to the original payment card.

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, the customer should be contacted and new details obtained.

6. TERMINAL SECURITY

Only approved devices and related components are purchased by the University to ensure compliance with the security requirements of PCI DSS. Any requests for new or replacement devices should be requested via Treasury. Treasury will be responsible for keeping the device list up to date and should be reviewed annually.

All devices must be inspected regularly, and as a minimum before the commencement of service. The purpose of inspecting PDQ devices is to identify signs of tampering at the earliest opportunity and so reduce the impact of fraud. Tampering can be in a physical form such as skimming devices or swapping of terminal, or a change in performance that may indicate the presence of malware. Staff at the PDQ device locations should maintain a log of these visual inspections. Finance will periodically undertake unannounced checks of PDQ devices at each location.

All discrepancies must be investigated, and the device disconnected and removed from service until the situation is resolved. All incidents should be reported to Treasury as detailed in the Device Inspection procedure.

PDQ devices used to process card payments must:

- Only be used by University staff trained and authorised to do so as part of their normal duties.
- Be protected from physical access by unauthorised users.
- Not be taken off site for testing, repair or used without approval from Treasury.

PDQ devices must be returned to Treasury when they are no longer required or the contract has ended. This ensures that the devices can be disposed of in a secure and appropriate manner.

7. INFORMATION SECURITY

The University will maintain a level of payment security that meets or exceeds the requirements of the PCI DSS standard. Both internal and external audit will be given full access to payment security activities and controls as required in order to maintain compliance.

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

Where possible, all systems used within the cardholder data environment will be protected against malware with anti-virus software that update automatically and cannot be removed or disabled by users.

Cardholder data storage will be kept to a minimum and be securely encrypted when in transit across a network and at rest.

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

If a staff member is in any doubt over whether there has been an incident, a call should be logged immediately via the IT helpdesk with as much information as possible and they will advise on the most appropriate course of action.

8. COMPLIANCE AND MONITORING

All payment card-processing activities of the University must comply with the PCI DSS standard. All staff must adhere to this policy (and supporting policies and procedures) to minimise the risk to both customers and the University. Any failure to comply will put the University at risk of fines and may result in the removal of permission to accept card payments.

Treasury, with support of IT services, will conduct regular checks to identify non-compliance.

This policy is reviewed at least annually to ensure it:

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

9. SUPPORTING PROCEDURES AND DOCUMENTATION

- **Cardholder Data Handling**
- **Data & Document classifications**
- **Device Configuration**
- **Device Inspection**
- **Device Management**
- **Malicious Software Detection**
- **Payment Security Awareness Procedure**
- **Payment Solution Procurement Procedure**
- **Rebate Fraud Procedure**
- **Supporting Device Configuration**

- **Suspected Incident Response**
- **Third Party Management**

The supporting procedures and documentation are available from Treasury.