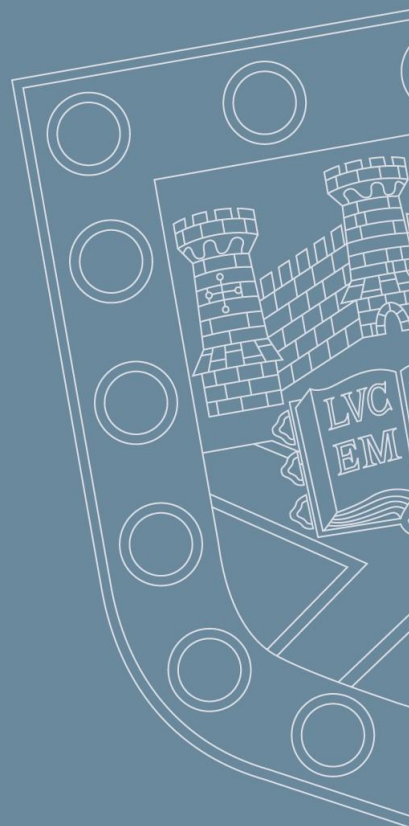




Payment Card Security Policy

Finance Services

Last Review and Update: 19th August 2026

Next Review: August 2027

CONTENTS

1. Introduction and Policy Statement
2. Online Payments
3. Card Payments
4. Additional Security Controls
5. Compliance and Review
6. Supporting Documents

1. Introduction and Policy Statement

- 1.1 The University's preferred method for taking individual payments for goods and services from students and former students, staff and visitors/partners is on-line via the customer's payment card (debit or credit card) and through a University approved compliant e-payment system.
- 1.2 Where essential due to the nature of the transactions, staff may use Point of Sale Terminals (PDQ)/card machines) but such machines must comply with the requirements set out below.
- 1.3 The Payment Card Industry Data Security Standard (PCI DSS) is a worldwide information security standard, created to help organisations that process card payments prevent card fraud. It requires strict control of data and confidentiality to ensure the security of payment card details. It is the global data security standard that any business of any size must adhere to if it wishes to accept card payments, and to store, process, and/or transmit cardholder data. The University is liable for fines should it fail to comply with PCI DSS as it is considered a breach of contract with our Bank. Non-compliance also puts confidential data held by the University at potential risk in contravention of the University's Data Protection Policy ([link](#)) and Data Protection Law.
- 1.4 Senior Managers are responsible for ensuring staff are aware of this policy, the associated procedures and that these are adhered to. Mandatory training is provided and should be undertaken annually by staff handling payment card transactions. This can be accessed via SIG PCI DSS E-Learning [LearnUpon](#).
- 1.5 If any member of staff identifies that this policy is compromised or is at risk of compromise then he/she must report the matter immediately to their line manager. They should feel able to do so in the case of genuine mistakes as well as if they are concerned about poor practice by others. The Head of Financial Operations in consultation with the line manager will decide on whether a further investigation is required or escalation to Deputy Director Finance Services.
- 1.6 Individual staff who do not comply with the requirements of the training and this set of policies and procedures may be subject to disciplinary action.

2. Online Payments

- 2.1 The preferred method of taking payment for goods and services is through the University Online Store or the Student online payment facilities on the Finance Services website <https://www.exeter.ac.uk/students/finance/makeapayment/>
- 2.2 Through the online payment system no card details are retained by the University and there is no access to full card details by any member of University staff as this information is stored on an encrypted external server maintained by the University's online payments service provider, WPM.
- 2.3 Refunds can only be processed by Financial Operations for that online payment system stated in paragraph 2.1.

- 2.4 The University approved supplier for all online payments is WPM. If staff need advice about setting up online payments, or if, in rare cases, an alternative supplier is needed, they should contact Head of Financial Operations to discuss their requirements. In this instance a copy of the suppliers up to date Attestation of PCI Compliance **must** be provided to the Head of Financial Operations in advance of implementation.

3. Card Payments

- 3.1 Where agreed (e.g. retail outlets), staff may take payments using a Point of Sale terminal. PDQ machines must be PCI DSS compliant. Financial Operations team are responsible for the approval of purchasing new machines of a specification approved by the University. Staff should not contact PDQ machine suppliers directly as the University must retain control over the machines in use to ensure compliance.
- 3.2 Payments using PDQ machines should normally be taken on a “customer present” basis. When a successful payment is processed the paper ‘merchant copy’ receipt generated by the machine should be stored securely in a locked draw/cabinet and the ‘customer copy’ handed to the customer. Receipts should not be retained if there is no business need to do so.
- 3.3 If the transaction is declined, the customer should be informed immediately and asked to contact the card provider. Receipts should be handled in the same way as in 3.2.
- 3.4 If the customer is not present and the online methods of payment is not suitable (for example loss of network connection), the customer may be asked to provide card details over the phone. These must be entered directly by the staff member taking the call into the PDQ machine. Normally this should be done immediately while the customer is on the phone and card details should not be written down. Staff should not store the card-validation code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions.
- 3.5 Confidential and sensitive information (e.g. card numbers) is never to be sent unencrypted through end-user messaging technologies such as e-mail, instant messaging, or chat. Card details should **never** be requested via email. **On no account** should card details be processed if received this way. Emails must be deleted out of the inbox and deleted folder and a new message composed to the customer informing them that their card details will not be accepted via email. Virtual keypad functionality delivered via WPM is in place for the Student Information Desk and Financial Operations to securely take card payments directly into the online system.
- 3.6 Card details should **never** be requested via a paper booking/payment form.
- 3.7 Refunds can only be processed by the staff member authorised to do so by Financial Operations Team. Refunds must be processed with the customer present and receipts should be handled in the same way as 3.2.
- 3.8 **Retention**
- Merchant copies of PDQ receipts must be kept for a rolling year of 12 months, for audit purposes. Merchant copies that have been held for 13 months or more can therefore be destroyed by confidential shredding. The receipts should be filed chronologically and in a secure environment.

A secure environment is defined as: within a safe, within a cash box, within a locked drawer

All of these should be stored in a locked room, where a log of access to the stored receipts must be maintained.

As and when card data needs to be destroyed, it must be destroyed in such a way that it cannot be reconstituted and the original data restored.

3.9 Physical Destruction - for physical paper copies of data

Staff must ensure:

- All paper based card data must be cross shredded, pulped or incinerated.
- Paper based card data must not be stored for recycling without first being cross shredded.
- If paper based card data needs to be stored prior to destruction, it must be securely stored in a lockable storage cabinet or container. A record of the items being stored must be kept and used to confirm prior to destruction that the items are present.
- If there is reason to suspect that paper based card data has been lost, stolen or compromised, this should be reported immediately to your line manager.

3.10 Destruction – Electronic / Digital

- In the advent that data is discovered in a digital format, it must be destroyed and deleted in such a way that it cannot be restored using forensic or data recovery tools.
- Digital data may occur on computers, backup tapes, hard drives, memory sticks, optical media (DVD/CD's).
- On discovery of a digital copy of card data, this should be reported to the PCI team ASAP to arrange secure destruction. Do not email, or copy the file. Note the filename, location and any dates associated with the file.
- Staff must establish the source of the data file and confirm if the file has been automatically or manually created.

4. Additional Security Controls

The University has incorporated additional security controls to ensure payment data is secure.

- 4.1 All members Finance Team will use University-issued devices, laptops or workstations, for all university related work especially financial.
- 4.2 Members of the Finance team with access to applications and software with financial information of the university, students and staff will have multi-factor authentication (MFA) enabled on their domain account.
- 4.3 Members of the Finance team with access to applications and software with financial information of the university, students and staff will have their domain password expire every 90 days which they will have to reset with appropriate complexity rules defined in the password policy (see Section 6 for the policy).
- 4.4 Members of the Finance team with access to applications and software with financial information of the university, students and staff will no longer be local administrators on their workstations or laptops.
 - 4.4.2 Any new software installation will require a request to IT. Any update to existing software installation is managed through Software Change Control Manager (SCCM) console.

- 4.5 Staff must ensure that payment card information, including full PAN numbers, must not be displayed or made visible to anyone except authorised staff. For example, payment equipment such as tills must not show the full PAN. (The first six and last four digits are the maximum number of digits that may be displayed.)
- 4.6 Staff must not store any payment card information in an electronic/digital format, whether or not encrypted, on any computers or storage devices whether by scanning, keying, photographing or any other means.

This applies to all types of payment card data including PAN, PIN, three-digit security codes and full track data. This requirement limits the University's scope so controls the cost, difficulty and feasibility of implementing and maintaining the PCI DSS controls that apply to storing card data necessary for compliance.

5. Compliance and Review

- 5.1 The University will undertake a PCI-DSS Compliance review on an annual basis. This will include a self-certification form being completed by Heads of Service and returned to the Head of Financial Operations by the date requested to ensure all areas of the University, with no exceptions, are PCI-DSS compliant.
- 5.2 All third party suppliers who provide card payment facilities must provide the Head of Financial Operations with an up to date copy of their Compliance to PCI DSS, on an annual basis.
- 5.3 The University will carry out regular vulnerability testing on the University network and the results will be notified to the PCI DSS Team.
- 5.4 The University will use and regularly update anti-virus software to protect the University network and its personal computers.
- 5.5 A University managed windows desktop must be used to access systems connected to the Card Data Environment (e.g. back office of e-payment facilities). Staff must never use a personal computer.
- 5.6 All individuals handling card data are expected to comply with all other University policies which cover security of data, and can be found at <https://www.exeter.ac.uk/ig/policy/>.
- 5.7 In the event that a member of staff suspects that there may have been a security breach, they should report this immediately to Data Protection Officer.

The PCI DSS incident team will be activated and must ensure that card processing is discontinued immediately and contact the appropriate external party.

6. Supporting Documents

- 6.1 This policy should be read in conjunction with the following University policies:

- [Firewalls Policy](#)
- [Encryption Policy](#)
- [Anti-malware Policy](#)
- [Access Management Policy](#)

Payment Card Security Policy

- [Password Policy](#)
- [Point of Sale PED Daily Check Policy](#)
- [Data Breach Policy \(including Procedure and Reporting\)](#)
- [PCI DSS - Third Party Service Provider Policy](#)