

**PCI DSS Policy**

1. **Introduction**
   1. This document supports implementation of the Payment Card Industry Data Security Standard (PCI DSS).
   2. 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.
   3. The standard was created to help organisations that process card payments prevent payment card fraud. The standard applies to all organisations that hold, process, or exchange cardholder information. This is achieved by the implementation of robust controls surrounding the storage, transmission and processing of cardholder data. Enforcement of compliance is carried out by the University’s acquirer (Worldpay) and ultimately the card providers, such as Visa and Mastercard. Organisations that fail to meet the compliance requirement risk losing their ability to process payment card payments and being audited and/or fined.
   4. Definitions
      * Payment card - A card backed by an account holding funds belonging to the cardholder, or offering credit to the cardholder such as a debit or credit card.
      * PCI DSS - The “Payment Card Industry Data Security Standard” (see above).
      * Stripe / track data - Information stored in the magnetic strip or chip on a payment card.
      * PAN - A “Primary Account Number” is a 16 digit number embossed on a debit or credit card and encoded in the card's magnetic strip which identifies the issuer of the card and the account.
      * PIN - A “Personal Identification Number” is a secret numeric password used to authenticate payment cards.
      * CVC2– 3-digit security code displayed on payment cards.
      * Cardholder Data – Payment card data including: Primary Account Number (PAN), name of cardholder, expiration date and service code.
      * Sensitive Authentication Data - Full magnetic stripe data or equivalent on a chip, CVC2 or PIN numbers.
      * PDQ Machine – A credit card swipe machine.
   5. This document includes statements on:
      * Scope
      * PCI DSS – 12 Requirements
      * PCI DSS Compliance Policy
      * Responsibilities
      * Card Processing
      * Retention of Cardholder Data
      * Physical Security - Card Processing Equipment
      * Contact Details
2. **Scope**
   1. The details contained in this policy apply to all staff who are responsible for processing payments made by debit or credit card.
3. **PCI DSS – 12 Requirements**
   1. The PCI Data Security Standard specifies twelve requirements for compliance, organized into six logically related groups called "control objectives". These are shown below;

|  |  |  |
| --- | --- | --- |
| **Control Objective** | **Item** | **PCI DSS Requirements** |
| Build and maintain a secure network | 1 | Install and maintain a firewall configuration to protect cardholder data |
| 2 | Do not use vendor-supplied defaults for system passwords and other security parameters |
| Protect cardholder data | 3 | Protect stored cardholder data |
| 4 | Encrypt transmission of cardholder data across open, public networks |
| Maintain a vulnerability management program | 5 | Use and regularly update anti-virus software on all systems commonly affected by malware |
| 6 | Develop and maintain secure systems and applications |
| Implement strong access control measures | 7 | Restrict access to cardholder data by business need-to-know |
| 8 | Assign a unique ID to each person with computer access |
| 9 | Restrict physical access to cardholder data |
| Regularly monitor and test networks | 10 | Track and monitor all access to network resources and cardholder data |
| 11 | Regularly test security systems and processes |
| Maintain an information security policy | 12 | Maintain a policy that addresses information security |

1. **PCI DSS Compliance Policy**
   1. All University card processing activities and associated technologies / systems must comply with PCI DSS.
   2. This document complies with Section 12 of the PCI DSS requirements (listed in Section 3 above) “Maintain a policy that addresses information security”.
   3. All staff involved in handling card payment data must be informed of the importance of cardholder data security as per the details held in this policy document.
   4. The PCI DSS policy shall be reviewed on a regular basis, such that changes in the regulatory environment are reflected in this document.
   5. Any University system that may involve the processing of card payments must be verified as being fully compliant with PCI DSS prior to use. The third party should be able to provide an Attestation of Compliance (AoC) as evidence that they have achieved compliance. These must be reviewed annually to ensure compliance is being maintained.
   6. This policy should be read in conjunction with the University Data Protection policy, which is a legal requirement under the Data Protection Act 1998. A breach of PCI DSS is highly likely to also be a breach of the Data Protection Act and may lead to penalties being imposed by the Information Commissioners Office (ICO).
2. **Responsibilities**
   1. Schools or Directorates must consult with the Financial Services Manager (Lee Bestwick) or the Information Security Manager (Simon Clements) before making any arrangements in respect of processing cardholder data. Any amendments to current practices must be compliant with PCI DSS regulations.
   2. Deans or Directors must nominate a member of staff who will be the Cardholder Data Security Champion for their faculty or Directorate. The nominated person will be responsible for the security of the cardholder data handled in their Directorate or Faculty and for ensuring that the contents of this policy are adhered to.
   3. The Cardholder Data Security Champion will be responsible for conducting an annual risk assessment of how cardholder data is handled in their Directorate or Faculty. The Financial Services Manager and the Information Security Manager will be able to advise and support the Payment Card Security Champion during the risk assessment process.
   4. The Cardholder Data Security Champion will be responsible for ensuring that staff who handle cardholder data in their Directorate or Faculty receive appropriate security training.
   5. The Finance & IDS Directorates are responsible for managing PCI DSS compliance for the University. Any payment processes that are deemed to be a potential risk will be stopped with immediate effect.
   6. Employees and other users who deliberately breach the terms of this policy may be subject to disciplinary action.
   7. Keele IT is responsible for arranging and assessing network security scans on a regular basis to ensure continued compliance with PCI DSS.
   8. The Finance Directorate is responsible for making sure that all relevant staff are aware of the sensitive nature of cardholder data and the associated risks.
   9. The Finance Directorate will ensure that service providers involved in processing card payments are PCI DSS compliant, and their compliance will be reviewed annually.
   10. All staff involved in handling card data must read and sign the “PCIDSS Guidance for Staff” policy to declare their awareness of PCI DSS and the steps that they must take to adhere to this policy. This declaration must be signed by all new starters and then on an annual basis to all staff involved in processing cardholder data. It will be the responsibility of the Cardholder Data Security Champion to ensure that all staff who handle cardholder data in their Faculty or Directorate sign the policy declaration.
   11. All staff involved in handling card data, should also complete the e-learning module available on Keele Learning Pool <https://keele.learningpool.com/> (search for “Payment Card Industry Data Security Standard” in the Course Directory.
   12. Staff using University systems that process cardholder data must not disclose their passwords or share user accounts.
   13. Staff involved in processing cardholder data must operate a “clear desk” policy where all sensitive material is removed from desks and stored away securely at the end of each working day or during periods where the desk is unattended.
   14. Staff must report any suspected breach or known potential risk as soon as possible to either the Financial Services Manager or the Information Security Manager, who will advise on what action should be taken.
3. **Card Processing** 
   1. Students should be encouraged to use the University’s online payment system (eVision) or the WPM system where possible.
   2. Staff must never request payment card details from a student or other third party via email or any similar end-user messaging technologies. Any details that are provided via email should be;
      * Deleted immediately from your email inbox and then deleted from the email recycle bin.
      * The customer should be informed of the inherent risk and that the payment will not be processed
   3. Staff must never send any cardholder details via email or any similar technology.
   4. No cardholder payment details should be stored electronically on spreadsheets, databases or other computer files under any circumstances. Any details currently stored must be deleted immediately.
   5. Sensitive cardholder data must not be recorded in written form. If this information must be written down to process a payment then the paper form must be destroyed by cross shredding immediately after processing. Storage of sensitive cardholder data is a breach of PCI DSS regulations. Sensitive cardholder data includes the PAN (16 digit card number) or the CVC2 code (3 digit security code). If the PAN is to be stored following payment then it must be encrypted or rendered unreadable (the last 4 digits are permitted to be visible).
   6. Cardholder data stored on paper (which must exclude sensitive data referred to in 6.5 above) must be stored in a safe or locked cabinet when not in use.
   7. Where paper copies of cardholder data must be transferred between locations on campus this must be hand delivered during office hours. Data of this nature must never be sent through the University internal mail system.
4. **Retention of Cardholder Data**
   1. Cardholder data should only be stored in paper form, and should exclude any sensitive authentication data (PAN or CVC2). Electronic copies of cardholder data should not be stored under any circumstances.
   2. Receipts are filed for a maximum period of 6 months to allow for verification of a disputed transaction by a customer.
   3. Receipts older than 6 months are disposed of securely by cross shredding.
   4. Receipts should only be stored in the Income Office unless prior agreement has been obtained from the Financial Services Manager. The Income Office storage facility also includes payments that have been processed by the Commercial and Residential Services team.
5. **Physical Security - Card Processing Equipment**
   1. All staff must be aware of the inherent risks surrounding the equipment used to process debit and credit card payments, this will apply equally to;
      * Processing payments through PDQ (Chip & Pin) machines
      * Processing through a Virtual Terminal (online system) on a PC or Laptop
   2. PDQ machines should only be operated by staff authorised and trained to use them.
   3. PDQ machines should be protected from the risk of tampering by being stored securely when not in use. They should be stored in a locked cabinet or in a room with access controls in place.
   4. PDQ machines should be subject to daily inspection to check for signs of tampering. It is recommended that the serial number is checked for verification purposes. Cabling and connections should also be checked for any signs of interference.
   5. PCs or Laptops that are used as Virtual Terminals should also be checked for signs of tampering. Cabling should be checked on a regular basis to ensure that there are no suspicious devices (such as hidden cameras or key loggers).
   6. PCs or Laptops that are used as Virtual Terminals should always be logged out of card processing systems or screen locked when the desk is left unattended.
   7. PDQ machines should only be Installed or maintained by the University preferred suppliers and by appointment only. Staff must always check the ID of the engineer before allowing access to the Terminals.
   8. Managers and staff should refer to the the “PCIDSS Guidance for Staff” policy for further information.
6. **Contact Details**

For further information on compliance with PCI DSS please contact:

Lee Bestwick Simon Clements

Financial Services Manager Head of Projects and Service Assurance

Direct Tel: 01782 734387 Direct Tel: 01782 734977

Email: [l.a.bestwick@keele.ac.uk](mailto:l.a.bestwick@keele.ac.uk) Email: [s.clements@keele.ac.uk](mailto:s.clements@keele.ac.uk)