Payment Card Data Security Policy

1 Introduction

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 standard was created to help organisations that process card payments reduce debit and credit card fraud through increased controls around transactions. It applies to all organisations which receive, process, store and exchange cardholder information, whether digitally or manually. Compliance is enforced by an organisation's merchant services provider on behalf of the major card brands. Organisations that fail to meet the compliance requirement risk losing their ability to process card payments and being audited and/or fined.

2 Scope

This policy covers the requirements for all payment card processing arrangements across the University, both manual and IT-based as well as all staff involved in processing card payments.

It is University policy that payment card data will only be processed in accordance with the conditions set out herein. Wherever possible, the processing of payment card data is undertaken by third party service providers who are licensed/accredited to process such data in line with the PCI DSS standard. The University seeks to eliminate all processing of credit card data through its IT infrastructure, transferring that responsibility and the PCI DSS compliance to the third party processor. The University will minimise the aspects of the PCI DSS standard to which it has to adhere, either by transferring the processing to an approved third party service provider, see Service Provider Policy (add link) or by eliminating business processes that require the processing of card data by the University.

3 Authorisation and Responsibilities

This policy is mandatory for all staff. Failure to comply with this policy may result in disciplinary action. Heads of Department are responsible for ensuring that their Staff are aware of the policy and that it is adhered to. Departments must not implement business processes that involve the processing of card payments without first consulting with IT Services, via the help desk, who will advise on how to proceed.

Line Managers are responsible for ensuring that all new and existing staff receive copies of relevant policies and training in PCI DSS requirements. A list of all staff currently authorised to routinely use devices to process payment cards, such as tills, PEDs, PDQ machines etc. must be maintained by the Department responsible for providing that service.

The Finance Office, supported by IT Services, is responsible for ensuring the University maintains PCI DSS compliance and will therefore remove any payment card processing activity causing unacceptable risk.

The Finance Office will maintain a current list of all University payment card service providers, see Service Provider Policy (add link).

IT Services is responsible for undertaking and assessing the results of the external and internal network security scans required for PCI DSS compliance. These scans must be run at least quarterly to check for security against external access to any networked devices that process payment card data and after any major systems changes.

IT Services is responsible for maintaining the inventory all devices used to process payment cards, such as tills, PEDs, PDQ machines etc.

In the event of there being a security breach of data, staff must follow the Incident Response Plan (add link). For any queries please contact the PCI DSS team at PCIDSSCompliance@warwick.ac.uk.

4 Payment Card Processing

Online Payment Processing

This is the preferred method for taking payment by credit or debit card as the approved payment service provider is responsible for handling the card holder data. No card details processed through an approved online system are retained by the University. Wherever possible students, staff and customers should be directed towards the University's online payment services and online payment pathway facilities - https://warwick.ac.uk/services/epayment

Customer Present Card Transactions

Where it is not possible to use online payment processing, the use of approved card processing terminals is permitted. Using Service Now, the IT Services team maintain an inventory of all authorised tills, PEDs and PDQ machines for card transactions. The inventory is reviewed and updated biannually by the relevant PCI DSS Contact Officer. Card payments can only be processed by one of these authorised devices. Line Managers are responsible for ensuring that the machines are not replaced, tampered with or adjusted in anyway without prior approval. See Section 5 for more information on terminal security.

Customer present card payments can be processed in two ways as follows:

- Using the EPOS systems, which have P2PE compliant terminals and are on separate VLAN's.
- Using standalone PDQ terminals which are connected via analogue lines and therefore do not use the network.

Card details must never be written down by any member of staff to use for a future payment attempt.

Customer Not Present Card Transactions

Request by Telephone

Where card details are provided during a telephone call, these must be processed directly into the PDQ machine at that time and must not be written down or noted anywhere. The card details must not be repeated back to the customer in such a way as to be audible to third parties. Card details must not be taken using a VOIP phone line as it is not a secure line.

If it is not possible to submit the card details immediately, then a call back must be requested or offered. Customer card details must not be entered into any system, web based or otherwise.

Card Details Received In Writing

The University's policy is to reduce and preferably eliminate the need for cardholder data to be held in paper form. Processes should be regularly reviewed to determine whether online processes can be implemented to replace paper based procedures.

Cardholder data (CHD) includes the primary account number (PAN) which is the full card number on the front of the card, the Cardholder name, the expiration date and the service code which restricts where the card can be used.

CHD is allowed to be stored for specified periods for regulatory and legal requirements and business use. However if stored the PAN must be rendered unreadable by methods such as hashing, truncation, and encryption. The full PAN must not be retained.

Sensitive authentication data (SAD) includes full track data which is stored on the magnetic strip, CAV2/CVC2/CVV2/CID number which is the 3 or 4 digit number usually found on the back of the card and the personal identification number (PIN).

SAD should never be stored after authorisation of the payment.

Receipt of CHD by email is a violation of PCI DSS as it is an unsecure channel and can therefore be intercepted. Any CHD received in this format must not be forwarded on and must be deleted immediately. Please ensure the data is also deleted from the email accounts deleted folder.

Receipt of CHD by fax is permitted if using an analogue line and the following processes are followed in relation to handling the data.

- The payment is processed immediately and the paperwork is destroyed by cross cut shredding. Please note SAD must not be recorded on paper.
- In a situation where it is not possible to process the transaction immediately then the details must be stored in a secure environment such as a locked drawer or cabinet and any movements documented prior to use. This is only to be actioned in exceptional circumstances.
- Any process that requires receipt and/or storage of CHD in paper form needs to be fully documented and approved by the Financial Controller.
- A log of staff members with access to cardholder data must be kept by the relevant department. Card payment details must not be kept for more than 6 months before being destroyed.
- The internal mail system must not be used to transfer paper CHD within the University.

Receipt of CHD by post is only permitted where detailed procedures provide evidence of strong mitigating controls. These procedures have to be approved by the University's Financial Controller and audited on an annual basis.

Storage of CHD on PC's in any format (email, access databases, excel spreadsheets, pen drives, etc.) is not permitted as it breaches the Security Standard Regulations and effectively makes the University non-compliant and could result in hefty fines from Visa and MasterCard. The most

common method of fraudsters obtaining card details is by hacking into computers which store CHD.

The University will conduct routine audits to ensure this Policy condition is being met.

5 Terminal Security

Only approved devices and related components are purchased by the University to ensure compliance with the security requirements for point of sale devices in line with PCI DSS. Any requests for new or replacement devices should be requested via the relevant PCI DSS Contact Officer, see appendix 1.

All terminals held by the University are logged in the University's PCI Devices Inventory via Service Now. The inventory should be updated for any known changes. The relevant PCI DSS Contact Officer is responsible for keeping the Inventory up to date and should be reviewed bi-annually.

Devices used to process payment cards, such as tills, PEDs and PDQ machines must:

- Only be used by staff trained and authorised to do so as part of their duties.
- Be protected from physical access out-of-hours by unauthorised users. Small devices such as PDQ's should be locked away wherever possible. Larger devices such as tills must be kept in areas with restricted access when not in use.
- Be subjected to routine visual inspection each day before use. Equipment, cabling and connections should be inspected for signs of tampering. It is the line manager's responsibility to ensure a log of visual inspections is kept.
- Not to be taken off site for testing, repair or use without express approval from the relevant PCI DSS Contact Officer (appendix 1).

Out-of-hours visitors to areas giving access to payment equipment must be supervised and details of such visits should be logged.

The installation of new or replacement equipment must be validated and approved by the Financial Controller in conjunction with IT services to ensure the security of payment equipment has not been compromised.

Payment devices must not be positioned where University CCTV cameras could record card numbers, pin numbers and/or secure card data.

The University will provide training for operators to ensure awareness of terminal security. The line manager will be responsible for ensuring all authorised operators complete the training.

6 Destruction of Cardholder Data

CHD must be securely deleted or destroyed if not needed for legal, regulatory or business use, with the aim of eliminating unnecessary storage of data. Given the University's card payment processes, it should not be necessary to store CHD.

Where data is stored before destruction, CHD must be locked in a secure area and access restricted. Details of team members that require access should be kept within the Department and there should be a documented process for keeping this information secure.

Audits will be conducted by the Finance Office to ensure CHD is not kept unless there is an approved and documented process for secure storage and data held does not exceed retention requirements.

Hardcopy materials must be shredded using a cross cut shredder and then disposed of in confidential waste, incinerated, or pulped so that CHD cannot be reconstructed.

All persons handling CHD must receive training on safe storage, retention and destruction of CHD as part of their induction pack/training module and the PCI DSS awareness module.

7 Compliance and Monitoring

All payment card processing activities of the University must comply with the PCI DSS. No activity or technology may obstruct compliance with the PCI DSS.

All Departments must adhere to this Policy to minimise the risk to both customers and the University. Failure to comply will render the University liable for fines and may also result in Visa and/or MasterCard preventing transactions from being processed by the University.

The Compliance team will meet regularly to ensure the University maintains compliance. They will conduct regular checks and audits of the University's systems and processes to identify non-compliance which could result in threats and vulnerabilities.

If you have any queries or compliance issues with any aspect of this policy, you should contact a member of the Compliance Team via PCIDSSCompliance@warwick.ac.uk.

Appendix 1

Contact Officer	**Departments**
Atia Chaudry – IT Systems Manager	Retail Outlets
Graham Yarrow – Application Management Specialist	Arts Centre and Sports Centre
Catherine Wallis – Financial Controller	Academic Departments, Conference Sales Departments and Service Support Departments