University of Liverpool

Card Payment Policy

Reference Number	FIN-001
Title	Card Payment Policy
Version Number	1.0
Document Status	Active
Document Classification	Public
Effective Date	03 June 2014
Review Date	03 June2015
Author	CSD (David Hill)/Finance (Ian Potts)
Approved by	Corporate Services & Facilities Committee
Implemented by	CSD/Finance
Monitoring of compliance	Faculty Information Security Managers (Local) CSD Information Security (Central) Central Finance officers
Comments	This Policy should be read in conjunction with the University ISMS, Information Security policy and sub policies. Includes Processing and Storage of Debit/Credit Card and Purchase Card data

Contents

1. Introduction

To combat fraud, all businesses handling card payment data are required to comply with new industry rules aimed at increasing data security. This Policy applies to all University members, departments and stakeholders throughout the University that handle Card Payment Data.

2. What is PCI-DSS? (Payment Card Industry Data Security Standards)

PCI-DSS is the global data security standard adopted by the payment card brands for all entities that process, store or transmit cardholder data. It consists of a number of steps and security best practices that help to ensure the secure processing of sensitive data throughout the University.

There are 12 requirements to PCI-DSS, these include:

Requirement No:	Requirement Summary
Requirement 1-2	Build and maintain a secure network
Requirement 3-4	Protect cardholder data
Requirement 5-6	Maintain a vulnerability management programme
Requirement 7-9	Implement robust control measures / Control access to card data
Requirement 10-11	Regularly monitor and test your computer networks
Requirement 12	Make information security a priority

For more information please refer to https://www.pcisecuritystandards.org/

Card Payment Data

Card payment data consists of 2 main sets of data that must be protected by the University at all times. These include:

<table>
<tr><th colspan="2">Card Payment Data</th></tr>
<tr><th>Cardholder Data</th><th>Sensitive Authentication Data (SAD)</th></tr>
<tr><td>Primary Account Number (PAN) i.e. the 16 digit number on the front of the card.</td><td>Full Magnetic Stripe Data/Chip Data</td></tr>
<tr><td>Cardholder Name</td><td>CAV2/CVC2/CVV2/CID i.e. the last 3 digits on the signature strip on the back of the card</td></tr>
<tr><td>Expiration Date</td><td rowspan="2">Pin Numbers</td></tr>
<tr><td>Service Code</td></tr>
<tr><td colspan="2">PCI DSS requirements are applicable if a primary account number (PAN) is stored, processed, or transmitted. If the PAN is not stored, processed, or transmitted, PCI DSS requirements do not apply.</td></tr>
</table>

3. Purposes of Policy

This policy deals with the acceptable use and the controls required for receiving, processing and storing information in respect to all card data and covers all electronic and manual handling methods, including:

- Face to face
- Telephone
- Internet

4. Responsibility

The management and control of information received in respect of cards at the University applies to all members that handle card payment data and any other data that is associated to legislation e.g. Data Protection Act.

The following procedures must be adhered to:

- Access to payment card transactions and data must be restricted to only those members of staff who need access as part of their role.
- Staff and any University members (where required) should be made aware of the importance and confidentiality of card payment data e.g. appropriate checks and mandatory training is undertaken prior to allowing access to card payment data
- It is strictly prohibited to **send, receive, process and store** card details by Unapproved University Methods.
- Merchant copies of payment receipts must be stored in a physical secure location and disposed of as confidential waste.

Card payment data **MUST NOT** be written down. This includes when taking payments over the phone. The details must be entered direct into the online payment screens. If for some reason the payment cannot be input immediately the caller's contact details should be taken and a call-back arranged.

5. Physical Security of IT equipment (PDQ's/Card Payment Processing Systems)

For more information about the use and security of IT equipment associated with card payment and sensitive data assets please refer to the Physical and Electronic Security Policy.

6. University Approved Card Payment Methods and Services

Card data must only be received and processed by the University approved methods and services. These are:

University Approved Payment Methods				
Payment Method	Approved Payment Services	Card Transaction	Mandatory Controls	Storage of Card Data
Customer Present	**Online**	**Web Application Transaction**	Payment via an online system should generate an email payment confirmation to the customer. This should be the only confirmation document received by the customer from the University for the transaction.	**No** **Data is held by the University PCI-DSS compliant approved supplier**
			If a customer's payment has been unsuccessful or declined, the customer should contact their card provider in the first instance.	
			If a customer faces difficulty in making a payment then staff assistance can be provided.	
			If the payment problem cannot be resolved, the customer should provide a number to be called back on at a suitable time or offered an alternative payment method.	
	EPOS/PDQ	**EPOS/PDQ**	When the customer is present the card should be processed through the PDQ/EPOS machine according to the machine instructions.	**ONLY merchant receipts held in physical secure storage**
			If the transaction is successfully processed, the merchant copy should be securely stored and the customer copy given to the customer.	
			If the transaction is declined, the customer should be advised immediately.	

			The option of paying with a different card should be offered.	
			The customer copy stating that the payment was declined should be given to the customer and the merchant copy should be stored securely.	
Customer NOT Present	**Telephone**	**PDQ/Web Application Transaction**	Where card details are provided during a telephone call, these must be processed directly into the PDQ or online payment system at that time. The card details must not be written down.	**No** **Data is held by the University PCI-DSS compliant approved supplier**
			When card details are being provided during a telephone call these must not be repeated back to the customer in such a way that it can be intercepted by third parties.	
			If it is not possible to submit the card details immediately then a call back must be offered.	

Approved PDQ machines and Third Party Suppliers

The University provides card payment processing terminals (PDQ's) and web application transaction solutions which are approved and are PCI-DSS compliant.

The terminals in use have been selected to ensure that appropriate controls are in place to minimise risk, for example, the number of PAN digits that appear on receipt rolls is limited to just the last four digits. Only PDQ terminals provided by the University's approved supplier (Barclaycard) should be used. Any queries about obtaining or upgrading a PDQ terminal should be directed to processing@liverpool.ac.uk.

The web application transaction solutions ensure that the relevant card payment data is securely processed and stored via a segregated secure transmission and storage solution with all relevant network controls. The University approved provider for online payments is WPM. WPM is PCI-DSS compliant and should be used for all such payments.

The use of any other providers for online payments will require:

1. Due diligence checks to be performed to ensure the prospective provider is PCI-DSS compliant.
2. Business case detailing why WPM can't be used.
3. Formal approval by the Director of Finance.

The authorisation of alternative providers will only be granted in exceptional circumstances and in the first instance the WPM option will be explored.

7. Unapproved Card Payment Methods

The following are unapproved methods of payment and should not be used:

- Post/Written
- Email
- Fax
- Voicemail/Recordings

Accepting cardholder data via the above methods exposes the University to non-compliance with the PCI-DSS. This may result in fines, reputational risk if there is a data breach and ultimately potential withdrawal of the facility to take payments by credit or debit cards.

Under no circumstances should the non-approved payment methods be used without a formal University review

In the event of receiving card payment data via an unapproved method the data should be disposed of securely once identified e.g. if a student emails card details the email should be deleted and the sender contacted to arrange payment by one of the approved methods.

8. Storage of Card Payment Data

In the event that storage is required for operational, regulative and legislative requirements, **ONLY** the data below can be stored:

- Primary Account number (PAN) – First 6 or last 4 digits only
- Cardholder Name
- Service Code
- Expiration Date

The approved methods are designed to securely store the relevant data for legislative requirements.

Below are only a few examples of further controls required and must be active at all times with the appropriate technology in place:

- Masking to ensure **ONLY the first 6 OR last 4 digits of the PAN** can be seen (relevant to displaying on computer screens/receipts/voicemail)
- Truncation, hashing and encryption via transmission and storage databases
- Segregation away from other data sources on a designated secure server
- Technical hardening and further controls of all aspects of systems, network and services used to process/store/transmit card payment data
- Technical vulnerability and penetration testing of services on a regular basis

9. Approved Payment PC's and area(s)

The University has taken all appropriate steps to ensure any risks to staff, students and payment services have been reduced and mitigated accordingly, to allow secure payments to be undertaken across the University and in line with regulative controls.

Staff must:

- use University PC's within secure staff offices/rooms to submit/process University customer card payments at all times
- not submit/process customer card payments via non- approved University offices/rooms at any time e.g. at home or connect to these services from a remote location
- direct students to the University online payments services in the first instance
- direct students wishing to make a payment via a University PC to the approved payment PC's and areas ONLY

Students must:

- use their own device (PC/Laptop/Tablet/mobile) to connect and submit card payments to University online payment services in the first instance
- in the event a student's account is barred, and/or a student wishes to make an online payment via a University PC, the student must attend the approved payment PC's and areas ONLY

10. Non-Approved Payment PC's and area(s)

Card payments that are submitted via non-approved University PC's and area(s) are at the staff/student's own discretion and by connecting to non-approved PC's/area(s) the individual accepts the risks that may occur.

11. Receipt Rolls

The customer copy must be returned direct to the customer. The merchant copy of the card terminal receipt roll must be stored securely in a locked location with access control or a log of access.

12. Refunds

All refunds must be returned using the original payment source and be made to the customer / student who made the original payment.

Where possible these should be returned to the card on which the original payment was made. The only permissible exception is where the card has expired or an account is closed. **Proof of this should be obtained**. In these circumstances refunds may be made to an alternative card held by the payee.

13. Problems with Payment Card Transactions

If a customer's payment has been unsuccessful or declined, the customer in the first instance should contact their card provider.

14. Secure Disposal

All assets that have the capability of storing card payment details must be disposed of in a secure manner. Please refer to the IT Asset Disposal Policy for more information.

15. Incident Management

In the event that an information asset is damaged, lost, or compromised it must be reported immediately to the CSD Helpdesk and to the relevant Faculty/Department Information Security Manager.

For more information on reporting information security incidents please refer to the Information Security Incident Response Policy.

16. Third Party Approved Suppliers

Any third party appointed to manage card holder data on behalf of the University must be an approved and trusted University partner.

The third party must be audited on an annual basis and PCI-DSS certification must be evidenced.

For more information please refer to the IT Procurement and Third Party Security Policy and Information Security Review Policy.

Appendix A (University ISMS)

- Regulations for the Use of IT Facilities at the University of Liverpool (incorporating the JANET Acceptable Use policy)
- Information Security Policy
- Data Protection Policy
- Physical and Electronic Security Policy
- Information Security Incident Response Policy
- Security Investigation Policy
- Information Security Review Policy
- Social Media Compliance Policy
- Records Retention Policy
- Risk Management Policy
- IT Asset Disposal Policy
- IT Procurement and Third Party Security Policy
- Student/HR Disciplinary Procedures

Relevant legislation includes:

- Data Protection Act 1998
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Computer Misuse Act 1990
- Copyright, Design and Patents Act 1988
- Copyright (Computer Programs) Regulations 1992
- The Terrorism Act 2000
- The Anti-Terrorism, Crime and Security Act 2001
- Official Secrets Acts 1911-1989
- Obscene Publications Act 1994

Relevant Regulation includes:

- PCI-DSS (Payment Card Industry Data Security Standards)