UNIVERSITY of STIRLING

CARD PAYMENT POLICY

May 2016

1. Introduction

All businesses that handle card payment data are required to comply with industry rules aimed at increasing data security. These are set out in the Payment Card Industry Data Security Standards ("PCI DSS"), which were developed by the five card brands: VISA, MasterCard, AMEX, JCB and Discover. The purpose of PCI DSS is to ensure that businesses are reducing the risk of card payment data theft and fraud and therefore providing a secure environment for their customers to make payment. The standard applies to all organisations that hold, process, or exchange cardholder information. Enforcement of compliance is via the organisations card provider. Organisations that fail to meet the compliance requirements risk losing their ability to process card payments and being audited and/or fined.

To reduce the University's exposure to compliance costs and the risk of non-compliance, the University seeks to eliminate all processing of credit card data – transferring that responsibility and the requirement to be PCIDSS compliant to an accredited third party processor. By doing so the University will be taking steps to minimise the aspects of the PCI DSS standard to which it has to adhere. Any University employee who comes into contact with cardholder data needs to be aware of PCI DSS, and how they as an individual can reduce the risk of cardholder data theft and fraud.

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

2. Purposes of Policy

The purpose of this policy is to set out the requirements of the PCI DSS in respect of the transmission, processing and storage of cardholder data, and the key responsibilities in connection with the achievement and maintenance of compliance with PCI DSS. It applies to all individuals and systems within the University that come into contact with cardholder data, whether these be electronic or paper based.

3. PCI-DSS Applicability to the University

The University is a 'Level 4 Merchant'[1] which means that certification to the Standard requires the completion of an annual self-assessment questionnaire (SAQ) to demonstrate compliance.

[1] Merchants are categorised by the payment card brands dependent on the number of card transactions they process each year.

The University's cardholder data environment requires completions of SAQ C[2] which requires implementation of a subset of the prescriptive controls that are required by the standard and detailed in appendix 1.

It is University Policy that normally no card data are to be held or stored by it. Unless an exception applies, all card data are to be processed by a level 1 accredited PCI DSS third party provider. Where card data is to be processed directly by the University, all such processing must be PCI DSS compliant

4. Definition of Cardholder Data

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

CARD PAYMENT DATA	
Cardholder Data	**Sensitive Authentication Data (SAD)**
Primary Account Number (PAN) i.e. the 16 digit number on the front of the card.	Full Magnetic Stripe Data/Chip Data
Cardholder Name	CAV2/CVC2/CVV2/CID i.e. the last 3 digits on the signature strip on the back of the card
Expiration Date	Pin Numbers
Service Code	

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**.**

5. Responsibility and internal control

The management and control of information received, in respect of cards at the University, applies to all employees 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:

[2] There are 6 SAQs within the scheme. Level 2, 3 and 4 Merchants select the most appropriate SAQ based on their cardholder data environment. Level 1 Merchants do not complete an SAQ but have to report on compliance annually.

- 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 retained in a secure, locked cabinet or room at all times and cross shredded immediately after use.

Due to the diverse nature of business within the University, operational procedures will be documented at a local level to incorporate these requirements. Further guidance is provided in appendix 2.

5. 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.	
			When the customer is present the card should be processed through the PDQ/EPOS machine according to the machine instructions.	

	EPOS/PDQ	**EPOS/PDQ**	If the transaction is successfully processed, the merchant copy should be securely stored and the customer copy given to the customer.	**ONLY merchant receipts held in physical secure storage**
			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.	

6. Approved PDQ machines and Third Party Suppliers

The University provides card payment processing terminals (PDQs) 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 (FEXCO) should be used. Any queries about obtaining or upgrading a PDQ terminal should be directed to banking@stir.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 Education Ltd ("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. 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.

6. Unapproved Card Payment Methods

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

- Post/Written
- Email
- 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

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.

7. 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

8. Approved Payment PCs 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.

To help make the statement in the previous paragraph valid, staff must:

- Use University PCs 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.

9. Non-Approved Payment PC’s and area(s)

It should be made clear that card payments that are submitted via non-approved University PCs and area(s) are at the staff/student’s own discretion and by connecting to non-approved PCs/area(s) the individual accepts the risks that may occur.

10. Receipt Rolls

The customer copy must be returned directly 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.

11. 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.

12. 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.

13. Secure Disposal

All assets that have the capability of storing card payment details must be disposed of in a secure manner.

14. Incident Management

In the event that an information asset is damaged, lost, or compromised it must be reported immediately to the Director of Finance.

15. 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.

Appendix 1 Applicable PCI-DSS Policy Requirements

The PCI-DSS defines the minimum criteria required for those processing card payments to become and remain compliant. This section outlines the minimum requirements which need to be implemented in order for a Level 4 Merchant to be compliant with the Standard in accordance with the requirements of SAQ C.

Requirement 1 Install and maintain a firewall configuration to protect cardholder data

Requirement 2 Do not use vendor-supplied defaults for system passwords and other security parameters

Requirements 1- 2 are not covered by this policy as the University employs 3rd parties to process online transactions securely

Requirement 3 Protect stored cardholder data

Requirement 4 Encrypt transmission of cardholder data across open, public networks

These sections are covered by this policy and primarily state that the University should not store or transmit card and transaction data unnecessarily. Organisations accepting payment cards are expected to protect cardholder data and prevent their unauthorised use.

Requirement 5 Protect all systems against malware and regularly update anti-virus software or programs

Requirement 6 Develop and maintain secure systems and applications

As for requirements 1- 2, these sections are not covered by this policy

Requirement 7 Restrict access to cardholder data by business need to know

Requirement 8 Identify and authenticate access to system components

Requirement 9 Restrict physical access to cardholder data

Requirements 7 – 9 are covered by this policy and deal with access to card data, which should be limited to when there is a business requirement and restricted to relevant staff only.

Requirement 10 Track and monitor all access to network resources and cardholder data

Requirement 11 Regularly test security systems and processes

As for requirements 1- 2, these sections are not covered by this policy

Requirement 12 Maintain a policy that addresses information security for all personnel