University of York Policy on the Management of Debit/ Credit Card Data

Version 1.0 25th February 2015

Index

1 Introduction and Policy Statement

1.1 The Payment Card Industry Data Security Standard (PCI DSS) is a worldwide information security standard, created to help organisations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise. It applies to all organisations which receive, process, store and pass cardholder information.

It is University Policy that credit card data will not be processed out with the conditions set out herein. It is University Policy that wherever possible, the processing of credit card data is sub-contracted to third-parties 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 infrastructure – transferring that responsibility and the requirement to be PCI DSS compliant to that third party processor. In this regard the University will take steps to ensure that it minimises the aspects of the PCI DSS standard to which it has to adhere, either by transferring that processing to a licensed third-party, or by eliminating business processes that require the processing of card data by the University.

The University is liable to fines from its merchant bank should it fail to comply with PCI DSS. This policy is required to ensure compliance with Section 12 of the Standard. This policy is mandatory to all staff. Failure to comply with this procedure may result in disciplinary action. Head 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 data without first consulting with IT Services and Finance, who will advise on how data are to be processed.

2 Security Breach of Data

2.1 In the event of there being a security breach of data, Staff must contact the Finance Compliance Officer – see Section 8, who will then make a decision on how to involve other parties. Credit card data is likely to be personal data as defined by the Data Protection Act 1998. Staff should contact the Compliance Officer (see Section 8) if a breach arises, as the University would also have to make a decision as to whether the UK Information Commissioner should be advised of a data breach.

3 Online Payments

3.1 In the first instance customers should make payment for goods and services online using the Online Payment Services and Online Payment Pathway facilities provided by the University. This is the preferred method and best practice for taking payments. For further information please see Section 8.

3.2 On completion of a successful payment the online system being used will automatically generate an email payment confirmation to the customer. This is the only Finance confirmation document that will be received by the customer for the payment.

3.3 If a customer's payment has been unsuccessful or declined, the customer in the first instance should contact their card provider. The most common reason for a declined transaction is the card provider suspecting the transaction may be fraudulent.

3.4 If a customer faces difficulty in making a payment then staff assistance can be provided. The customer should be assisted at the time of the enquiry, whether this is in person or via the telephone. If the payment problem cannot be resolved, then the customer should provide a number to be called back on at a suitable time.

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

3.6 For all card details which are processed through an online system, no card details are retained by the University.

4 Card Processing Terminals - Chip and Pin

4.1 Obtaining a Chip and Pin Machine

4.1.1 To request a Chip and Pin machine for your Department, please refer to Section 8.

4.1.2 To set up your Chip and Pin machine please follow the instructions that are provided by our Merchant Bank and are included with the machine.

4.2 Use of Chip and Pin Machine

4.2.1 Chip and Pin machines can only be connected to the secure FM network.

4.2.2 Chip and Pin payments should be processed for customer present transactions only. If the customer is not present then the Online Payment Services should be used for the payment.

4.2.3 One way for criminals to obtain card data is by tampering with the Chip and Pin terminals by adding equipment that reads cardholder data as the payment is being processed. This is called skimming. It is important to ensure that terminals are not tampered with. Portable terminals should be kept out of reach of customers and the public, and stored securely out of hours. You should be able to recognise if a terminal has been tampered with by comparing it against a reference photo. If you think your terminal may have been tampered with, stop using it and alert your manager immediately.

4.3 Customer Present With Card

4.3.1 When the customer is present the card should be processed through the Chip and Pin machine according to the machine instructions.

4.3.2 If the transaction is successfully processed, the merchant copy should be stored securely (see Section 5) and the customer copy given to the customer.

4.3.3 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 (see Section 5).

4.4 By Telephone by Cashiers in Financial Services only

4.4.1 Where card details are provided during a telephone call, these must be processed directly into the Chip and Pin machine direct or Online Payment Services at that time and must not be written down or noted anywhere.

4.4.2 When card details are being provided in a telephone call these must not be repeated back to the customer in such a way as to be audible to third parties.

4.4.3 If it is not possible to submit the card details immediately then a call back must be requested or offered. Please refer to Section 3.5.

4.4.5 Customer card details must not be entered into any system, web based or otherwise.

4.5 Card Details Received In Writing

4.5.1 Some customers may provide their card payment information in writing for processing i.e. by fax, in a letter, email or by booking form. Customers should be deterred from providing the information in this manner as it is not secure and there is no guarantee that these details have not been intercepted prior to being received by the University.

4.5.2 When details have been received by this method they must be processed immediately upon receipt.

4.5.3 Once the payment has been successfully authorised, the original document showing the full card details must be cross cut shredded. If the details have been received by email then the email must be deleted from the Inbox and the Deleted mail folder. If the email requires a response, the card information provided should not be contained within the reply.

4.5.4 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. This is only to be actioned in exceptional circumstances.

4.6 Chip and Pin Records

4.6.1 If the transaction is successfully processed, the merchant copy should be stored within the till drawer or cash box for the duration of the working day. The customer copy must be sent to the customer.

4.6.2 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 sent to the customer and the merchant copy should be stored within the till drawer or cash box for the duration of the working day. When storing merchant copy receipts these must be treated as a confidential document and should be marked accordingly.

4.6.3 The Chip and Pin machine transaction slips are to be sorted into card type and must be reconciled to the Chip and Pin report at the end of business each day. The Chip and Pin report should then be sent to the Finance Services Cash Office at Market Square in a sealed envelope clearly marked Private and Confidential. The envelope seal should be signed by the staff member from the Department who was responsible for the reconciliation.

4.6.4 Merchant copies of Chip and Pin 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.

5 Card Details Received in Writing

This Policy prohibits the storage and retention of credit card data by and within the University. The University will conduct routine audits to satisfy itself that this Policy condition is being met.

5.1 Storage of card details on PC’s in any format (email, access databases, excel spreadsheets, pen drives, etc.) 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 stores cardholder information.

5.2 Safe and secure storage is defined as:
Within a safe or
Within a locked Cash Box or
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.

5.3 Merchant copies of Chip and Pin receipts must be retained by the University within each relevant Department 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 merchant copy receipts are to be filed chronologically and stored in a secure environment as detailed in Section 5.2.

6 Refunds

Online Refunds

6.1.1 The refund must be approved by an authorised signatory for the cost centre and then passed to Finance Services Cash Office. The appropriate system is accessed and the refund is processed back to the source card from which the original transaction was authorised.

6.1.2 If a transaction is older than 180 days, a refund cannot be processed on to the source card for the original transaction. This is due to security measures implemented by the Payment Service Provider (PSP). In this instance the customer should be contacted for alternative details for the refund to be processed by BACS.

Chip and Pin Refunds

6.2.1 Chip and Pin refunds require to be authorised on the Chip and Pin machine using a

“Supervisor Card”. This card must be kept securely by an authorised signatory.

6.2.2 The refund must be approved by an authorised signatory for the cost centre. The refund should then be processed through the Chip and Pin machine back onto the source card from which the original transaction was authorised.

6.2.3 If the source card is unavailable for the refund to be processed then the customer should be contacted for alternative details for the refund to be processed by BACS. A refund must never be processed onto a card that is not the source transaction card.

7 Compliance and Monitoring

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

7.2 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.

7.3 A third party company is under contract to monitor University compliance with PCI DSS through annual Self-Assessment Questionnaire (SAQ) reviews.

7.4 Through regular meetings with relevant staff the Financial Accountant and Compliance officer will conduct regular checks that identifies threats, and vulnerabilities, and results in a formal risk assessment.

7.5 The University may screen potential employees to minimize the risk of attacks from internal sources.

7.6 The University will contractually require all third parties with access to cardholder data to adhere to PCI DSS requirements. These contracts will clearly define information security responsibilities for contractors. The University will also pass responsibility (contractually) for the upholding of the seventh data protection principle where personal data is passed to a third party for processing.

7.7 If you have difficulties implementing or complying with any aspect of this policy, you should contact the appropriate member of University staff – see Section 8

8 POINTS OF CONTACT

Online Payments web pages, including PCI-DSS and guidance on using online payment systems:

https://www.york.ac.uk/staff/finance/payments/

Financial Accountant and Compliance Officer:-
Ian Smallwood, ian.smallwood@york.ac.uk, 01904 322123

Financial Services, Cash Office, cash-office@york.ac.uk, 01904 322116
(for telephone payments and requests for chip and pin machines)

Finance Systems Support, finance-support@york.ac.uk, 01904 324095

IT Services, Richard Fuller, itsupport@york.ac.uk, 01904 323838

Appendix 1 - version history

1. Version 0.1 created 8th January 2014
2. Version 0.2 updated 28th October 2014
3. Version 1.0 agreed by PCI-DSS team 26th February 2015
2. Next review point: April 2017 (every three years)