Payment Card Security Policy and Procedures

Adherence to this policy and the associated procedures is mandatory for all staff who handle or process card payments on behalf of the University.

1. Introduction and Policy Statement

1.1 The University's preferred method for taking individual payments for goods and services from students and former students, staff and visitors/partners is on-line via the customer's payment card (debit or credit card) and through a University approved compliant e-payment system.

1.2 Where essential due to the nature of the transactions, staff may use Point of Sale Terminals (PDQ or card machines) but such machines must comply with the requirements set out below.

1.3 The Payment Card Industry Data Security Standard (PCI DSS) is a worldwide information security standard, created to help organisations that process card payments prevent card fraud. It requires strict control of data and confidentiality to ensure the security of payment card details. It is the global data security standard that any business of any size must adhere to if it wishes to accept card payments, and to store, process, and/or transmit cardholder data. The University is liable for fines should it fail to comply with PCI DSS as it is considered a breach of contract with our Bank. Non-compliance also puts confidential data held by the University at potential risk in contravention of the University's Data Protection Policy (link) and Data Protection Law.

1.4 Deans of Schools and Heads of Professional Services are responsible for ensuring staff are aware of this policy, the associated procedures and that these are adhered to. Mandatory training is provided and should be undertaken annually by staff handling payment card transactions. This can be accessed via LEARN PCI DSS E-Learning.

1.5 If any member of staff identifies that this policy is compromised or is at risk of compromise then he/she must report the matter immediately to their line manager and the PCI DSS Team (pcidss@lboro.ac.uk). They should feel able to do so in the case of genuine mistakes as well as if they are concerned about poor practice by others. The PCI DSS team in consultation with the line manager will decide on whether a further investigation is required.

1.6 Individual staff who do not comply with the requirements of the training and this set of policies and procedures may be subject to disciplinary action.

2. Online Payments

2.1 The preferred method of taking payment for goods and services is through the University Online Store or the Student online payment facilities on the Finance Office website (accessible through Learn).

- Online Store contact: online.store@lboro.ac.uk or it.services@lboro.ac.uk
- Online student payments contact: Finance Shared Services on 222030

2.2 If at all possible, payments should be taken by directing the individual to use one of the services above and staff will not therefore have any access to the individual's payment card details.

2.3 PCI DSS requires that the customer has a free choice of which device to use to make their on-line payment. Staff should therefore not pro-actively direct customers to a specific computer or other device to make payments. However, if the customer asks to use a University device staff may indicate that they may do so. In a small number of cases, devices have been set up with additional security (e.g in Student Enquiries) and relevant staff may direct individuals to use this machine.

2.4 Through the online payment system no card details are retained by the University and there is no access to full card details by any member of University staff as this information is stored on an encrypted external server maintained by the University's online payments service provider, WPM.

2.5 Refunds can only be processed by the designated service for that online payment system stated in paragraph 2.1.

2.6 The University approved supplier for all online payments is WPM. If staff need advice about setting up online payments, or if, in rare cases, an alternative supplier is needed, they should contact pcidss@lboro.ac.uk to discuss their requirements. In this instance a copy of the suppliers up to date Attestation of PCI Compliance **must** be provided to the PCI Team in advance of implementation.

3. Card Payments

3.1 Where unavoidable (e.g. retail outlets), staff may take payments using a Point of Sale terminal (PDQ machine). PDQ machines must be PCI DSS complaint. To check the machine you are using is compliant please contact the PCI team on pcidss@lboro.ac.uk. The team can also advise on the purchasing of new machines of a specification approved by the University. Staff should not contact PDQ machine suppliers directly as the University must retain control over the machines in use to ensure compliance.

3.2 Payments using PDQ machines should normally be taken on a "customer present" basis. When a successful payment is processed the paper 'merchant copy' receipt generated by the machine should be stored securely in a locked draw/cabinet and the 'customer copy' handed to the customer. Receipts should not be retained if there is no business need to do so.

3.3 If the transaction is declined, the customer should be informed immediately and asked to contact the card provider. Receipts should be handled in the same way as in 3.2.

3.4 If the customer is not present and the online methods of payment noted in paragraph 2 above are not suitable (for example loss of network connection), the customer may be asked to provide card details over the phone. These must be entered directly by the staff member taking the call into the PDQ machine . Normally this should be done immediately while the customer is on the phone and card details should not be written down. Only if there is a genuine reason why the transaction cannot be processed immediately (loss of network) may details be written down. They must be stored securely in a locked drawer/cabinet, actioned as soon as possible and then **cross shredded**. Do not store the card-validation code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions.

3.5 Confidential and sensitive information (e.g. card numbers) is never to be sent unencrypted through end-user messaging technologies such as e-mail, instant messaging, or chat) Card details should **never** be requested via email. **On no account** should card details be processed if received this way. Emails must be deleted out of the inbox and deleted folder and a new message composed to the customer informing them that their card details will not be accepted via email. Please follow the processes in the PCI Awareness Document on LEARN on how to delete the emails.

3.6Card details should **never** be requested via a paper booking/payment form.

3.7 All confidential and sensitive data will be retained only as long as required for legal, regulatory and business requirements and in a secured location (e.g. locked cabinet/safe). Cardholder “authorization data”, including track, CVV2, and PIN information, will be retained only until completion of the authorization of a transaction. After authorization, the data must be destroyed via cross shredding or pulping by using the University approved confidential waste service. Storage of cardholder authentication data post-authorization is prohibited..

3.8 The retention period for cardholder data is **3 months**, unless otherwise approved. Schools and Professional Services must ensure there is a quarterly process in place to remove cardholder data that exists past the retention period.

3.9 Refunds can only be processed by the staff member authorized to do so by the School or Service (Supervisor) using a Supervisor card and secure password. Refunds must be processed with the customer present and receipts should be handled in the same way as 3.2.

3.10 Supervisor cards must be stored in a securely locked drawer/cabinet out of sight and only used by the authorised staff member detailed in 3.10 above.

4. Compliance and Review

4.1 The University will undertake a PCI-DSS Compliance review on an annual basis. This will include a self-certification form being completed by Deans and Heads of Professional Services and returned to the Finance Office by the date requested to ensure all areas of the University, with no exceptions, are PCI-DSS compliant.

4.2 Members of the PCI-DSS team will do annual and ad hoc spot checks on all PDQ machines and payment methods.

4.3 All third party suppliers who provide card payment facilities must provide the PCI Team with an up to date copy of their Compliance to PCI DSS, on an annual basis.

4.4 The University will carry out regular vulnerability testing on the University network and the results will be notified to the PCI DSS Team.

4.5 The University will use and regularly update anti-virus software to protect the University network and its personal computers.

4.6 A University managed windows desktop must be used to access systems connected to the Card Data Environment (e.g back office of e-payment facilities). Staff must never use a personal computer.

4.7 All individuals handling card data are expected to comply with all other University policies which cover security of data, and can be found at http://www.lboro.ac.uk/services/registry/information-governance/ .

Version Control

Version	Revision Date	Summary of Changes	Approvals
1.0	June 2016	Initial draft created	PCI Project Team
2.0	September 2016	4.4 amended	PCI Project Team
3.0	October 2016	Renaming of Policy	PCI Project Team
4.0	November 2016	Minor wording changes	PCI Project Team
5.0	February 2017	Removal of individual email addresses, minor wording amendments to ensure continuity	To IGSC for Approval
6.0	March 2017	Minor wording changes as per feedback from IGSC. Training moved to section 5	To IGSC for Approval
7.0	5 July 2017	Major re-ordering and rewording to improve clarity and remove repetition	For further iteration between JCN, Jo and Carol for sign off by JCN under chairs action for IGSC
8.0	10 July 2017	Further minor revisions by Jo Brewin and Jennifer Nutkins	
9.0	Nov 2017	Addition of Data Retention Period and disposal – point 3.7-3.8	NK/ML
10.0	Nov 2017	Amendment of text to fit with PCI requirements in points 3.4, 3.5.and 3.7	IGSC – Chair’s Action