

**Processing Debit / Credit Card Payments - Data Security**

**Why is it important?**

PCI DSS is the Payment Card Industry Data Security Standard. This is a worldwide standard that was set up to help businesses process card payments securely and reduce card fraud. We need to take great care over the storage, transmission and processing of cardholder data that we handle.

**What do we need to do?**

The aim must always be to protect sensitive cardholder data and guard against fraudulent or criminal activity.

**How do we do this?**

* Access to Chip & Pin terminals should be restricted only to staff authorised to use them on behalf of the University.
* Staff must never share their logon details with anyone.
* Terminals should be inspected regularly to check for evidence of tampering.
* The Card should never be taken out of sight of the cardholder.
* Cardholder details should not be written down unless absolutely necessary. They should not be saved on a spreadsheet or computer file for use at a later date or put in an email. Once the payment has been processed the details must be destroyed immediately and securely by cross shredding. The Card Security Code (CSC) on the reverse of the card should NEVER be written down.
* Staff must never ask customers to submit payment card details in an email. If staff do receive an email containing payment card details the email must be deleted immediately and then further deleted from the email recycle bin.
* Staff responsible for taking card payments should be properly trained when starting the job.
* Staff should have refresher training on an annual basis on cardholder data security
* Terminals should be stored securely when not in use
* All Terminals should only be Installed or maintained by the University preferred suppliers and by appointment only. Staff must always check the ID of the engineer before allowing access to the Terminals.
* Staff should take additional care if the payment transaction requires a signature. The Chip & Pin Terminal may occasionally instruct you to ask the payer to provide a signature authorisation;
* Make sure the card is not damaged, cut or defaced in any way
* Check the signature strip for signs of damage or tampering.
* Staff should know what to do in the event that card that should be retained -

Advise the customer that the bank has formally requested for the card to be retained. You are therefore obliged to do so and the customer will need to speak with their bank. Please contact a member of the Income Office Team or the Financial Services Manager for further information. In the event that the cardholder becomes threatening or abusive please call the Security Team immediately on extension 33004.

* Refunds should only be only be made by authorised persons. The refund should always be processed back to the original card that payment was made from and only after the customer has produced proof of purchase (the original receipt). Refunds should never be made in cash if the original payment was made by debit or credit card.
* If for any reason you are unsure about processing a payment you can make a “Code 10 Call”

This is actioned by pressing “10” on your Chip & Pin Terminal and then calling the Worldpay Authorisations team on 0845 7600 500. They will talk you through the process.

* Staff should be aware of the procedure for reporting a suspected security breach -

Please contact a member of the Income Office Team or the Financial Services Manager who will advise what action should be taken.

**What Learning Resources are available?**

* The University has developed a short e-learning module for key staff to gain a greater understanding of PCIDSS. The module takes approximately 15 minutes to complete.
* The module is available via the Keele Learning Pool <https://keele.learningpool.com/> (search for “Payment Card Industry Data Security Standard” in the Course Directory).

**Who can I contact for assistance?**

* Please contact your supervisor or line manager in the first instance.
* If further help is required please contact the Financial Services Manager or a member of the Income Office Team

………………………………………………………………………………………………………………..

**Declaration by Employee**

I confirm that I have read and understand the guidance shown above (Please tick the box below).

|  |
| --- |
|  |

I confirm that I will act in accordance with University guidance on cardholder data security (Please tick the box below).

|  |
| --- |
|  |

I confirm that I have completed the e-learning module for PCIDSS available on the Keele Learning Pool (Please tick the box below).

|  |
| --- |
|  |

|  |  |
| --- | --- |
| **Signed:** |  |
| **Print Name:** |  |
| **Date:** |  |