**PCI DSS Compliance guide**

***Introduction***

In order to be able to accept payment by debit and credit card, the University and subsidiaries must meet the requirements defined in the Payment Card Industry Data Security Standard (“PCI DSS”). PCI DSS is a worldwide information security standard defined and published by the Payment Card Industry Security Standards Council. The standard was created to help organisations that process card payments reduce the risk of payment card fraud through increased controls around cardholder information and its exposure to compromise. The standard applies to all organisations that store, process, or transmit cardholder information. Organisations that fail to meet the compliance requirements risk losing their ability to process payment card payments and/or fines.

Our customers and the public generally, expect the University to protect data on credit and debit cards. PCI DSS doesn't guarantee that there won't be a data breach, but it encourages the University to think wisely about how we use and store customer data.



**What is PCI DSS?**

PCI DSS is a set of 12 basic security requirements. It was put in place to ensure that businesses storing, transmitting or processing card data are not putting their customers or their businesses at risk of data theft and fraud.

**Why does the University need to be PCI DSS compliant?**

* Possible penalties for not complying with PCI DSS :
* An increase in security auditing (£cost)
* Facing an unlimited amount of fines,
* Significantly, losing the ability to process card transactions altogether (imagine this happening during Registration!)
* The reputation of the University is also at risk if there is a data breach.

**How do we keep the University PCI DSS compliant?**

Staying PCI DSS compliant could be a costly and time-consuming process as the more the University is involved with handling card data, the more open to abuse it is. However, there are some simple ways to reduce the cost and burden of compliance, and of course our risk of a data breach.

One of those ways is to avoid handling card data in the first instance. Please see note below on the Universities e-store capability.

**University E-Store (**[**estore.manchester.ac.uk**](file:///C%3A%5CDocuments%20and%20Settings%5Cmtfssmba%5CLocal%20Settings%5CTemporary%20Internet%20Files%5CContent.Outlook%5CA78ANVSD%5Cestore.manchester.ac.uk)**)**

The University already has payment pages - **eStore** - hosted by a PCI DSS compliant payment service provider available at [**estore.manchester.ac.uk**](file:///C%3A%5CDocuments%20and%20Settings%5Cmtfssmba%5CLocal%20Settings%5CTemporary%20Internet%20Files%5CContent.Outlook%5CA78ANVSD%5Cestore.manchester.ac.uk) where payments to the University can be made securely for products and services.

**eStore** can be used for selling conferences, short courses, events and products. Please access the website to see the diversity of products and services we already deliver and discover how you can exploit this resource. We already sell a wide range of products and services all around the world in a secure, quick and efficient manner, reducing administrative overheads locally.

Below is a summary of what eStore can offer:

Products and Services Made Simple:

* Collect deposits and balances for student field courses.
* Provide an easy route for payments of exam re-sits, resubmission fees, fines and memberships.
* Sell physical products to customers within the university and around the world.
* Option to send dispatch emails for physical goods.
* Allows an open amount for the customer to fill in.

Event Management:

* Give your delegates a choice of early-bird, standard, and concessionary fees.
* Add optional extras such as dinners, trips and accommodation.
* Collect registration info and add your own bespoke questionnaire.
* Display a conference image.
* Generate delegate lists.

Short Courses:

* Easily register students for your non-credit bearing courses.
* Allow payments for multiple delegates in one transaction.
* Add mandatory or non-mandatory extras.
* Display multiple instances of recurring courses.

Things to be aware of:

* The eStore is only for customers who are paying by card - sales invoicing, cheques or bank transfers have to be handled separately.
* All new store requests have to be approved by the VAT office.