University Policy for maintaining the security of credit/debit card data

<table>
<thead>
<tr>
<th>Author</th>
<th>C Milne / E Gillespie</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved by</td>
<td>University ICT Strategy and Planning Group</td>
</tr>
<tr>
<td>Approval date(s)</td>
<td>April 2015</td>
</tr>
<tr>
<td>Review date</td>
<td>April 2017</td>
</tr>
<tr>
<td>Version</td>
<td>1.0</td>
</tr>
<tr>
<td>Document type</td>
<td>Policy</td>
</tr>
<tr>
<td>Activity/Task</td>
<td>Information security</td>
</tr>
<tr>
<td>Keywords</td>
<td>PCIDSS</td>
</tr>
<tr>
<td>Document location</td>
<td></td>
</tr>
<tr>
<td>Confidentiality</td>
<td>PUBLIC</td>
</tr>
<tr>
<td>Version Number</td>
<td>Purpose / Changes</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>0.1</td>
<td>First draft for peer review (internal and external QSA)</td>
</tr>
<tr>
<td>0.2</td>
<td>Minor revisions made – linkage with wider finance policy and regulations noted</td>
</tr>
<tr>
<td>0.3</td>
<td>Minor revisions made</td>
</tr>
<tr>
<td></td>
<td>Draft circulated to University ICT Strategy and Planning Group</td>
</tr>
<tr>
<td>1.0</td>
<td>Policy approved – University ICT Strategy and Planning Group</td>
</tr>
</tbody>
</table>
### Table of contents

1. Introduction ................................................................................................................. 4
2. Policy objectives and scope ......................................................................................... 4
   2.1. Intended audience ................................................................................................. 4
   2.2. Where the policy applies .................................................................................... 4
   2.3. Policy statement ................................................................................................. 5
   2.4. Relationship with existing University Policy and Regulation ......................... 5
3. Implementation ............................................................................................................. 5
   3.1. Verification of the credentials/certification of third-party PCI-DSS level 1 providers 5
   3.2. Assessment of card data processing requirements and implementation of acceptable working practices ................................................................. 5
   3.3. Internal audit and review (compliance with this policy) .................................. 5
   3.4. PCI-DSS certification: in-house processing of card data .................................. 5
   3.5. Training ............................................................................................................ 6
4. Responsibilities ............................................................................................................ 6
   4.1. Finance ............................................................................................................. 6
   4.2. IT Services ....................................................................................................... 6
   4.3. Heads of School/Units and card data business process owners ....................... 6
5. Review ......................................................................................................................... 6
6. Policy breaches ............................................................................................................ 6
   6.1. Failure to process card data in a manner that is PCI-DSS compliant .................. 6
7. Sanctions ..................................................................................................................... 7
8. Availability ................................................................................................................... 7
9. Contacts/further information ......................................................................................... 7
1. Introduction

Where organisations process credit and debit card data (“card data”) to take payment for goods/services, there is a requirement to protect card data from theft and/or fraudulent use. The measures that organisations are required to have in place to protect card data are set out in the Payment Card Industry Data Security Standard (“PCI DSS”). This is an actionable framework for developing a robust card data security process - including prevention, detection and appropriate response to security incidents.

Being PCI DSS compliance signals that an organisation is doing its best to secure card data. There are significant costs in securing and maintaining compliance with PCI DSS. It is not cost effective for the University to process card data in house. To control that cost the University will use wherever possible card processing services provided by PCI DSS accredited third-party providers.

This policy seeks to minimise the number of occasions when card data is processed by the University to take payment for services/goods. Where it is necessary for the University to process card data, this policy requires that the appropriate security measures are in place, so that that processing is PCI DSS compliant.

The University is liable for fines from its Merchant bank should it process card data outwith the PCI DSS standard or any agreement on processing reached between both parties on agreed alternative arrangements. To reduce its exposure to compliance costs and the risk of monetary and reputational penalty from non-compliance, the University seeks to eliminate all processing of credit card data – transferring that responsibility and the requirement to be PCI DSS 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 to.

2. Policy objectives and scope

The objectives of this Policy are to:

- Ensure that no card data are held/stored by the University;
- Look to eliminate all forms of card data processing by the University, through transferring that responsibility to a certified PCI DSS level 1 third party processor;
- Ensure that any in-house card data processing remains by exception and that those process are and remain PCIDSS compliant; or
- Where is not possible to process card data in-house within the scope of the PCIDSS standard, then an agreement between the University and the appropriate Merchant Bank must be reached on alternative processing measures and that these are put in place before such processing can commence.

2.1. Intended audience

This Policy applies to all Heads of School/Unit and business process owners, where their processes involve the use of card data.

2.2. Where the policy applies

This Policy applies to all locations and instances where:

- Where the University is responsible for processing card data to receive payment for services/goods.

Please note, this Policy is not concerned with the use of University corporate credit cards. Separate University policy exists to support that aspect of card management.
2.3. **Policy statement**

It is University Policy that 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 (or equivalent) PCI DSS third-party provider. Where card data is to be processed directly by the University, all such processing must be PCI DSS compliant, or if this is not possible that alternative processing arrangements between the University and its Merchant Bank are negotiated, agreed and implemented.

2.4. **Relationship with existing University Policy and Regulation**

This Policy provides overall direction and support as to how card data will be processed by the University. This policy should be read in conjunction with relevant finance and monetary strategy and policy, and policies that provide direction on information security. Relevant University policy and currently includes:

- The University Information Security Policy (2011);
- Student and staff Codes on the collection and use of personal and sensitive personal data (revised annually); and
- Payment Acceptance Strategy (draft).

3. **Implementation**

3.1. **Verification of the credentials/certification of third-party PCI DSS level 1 providers**

The University will secure independent verification of the credentials/certification that a third party provider has the necessary qualification to provide PCI DSS processing services. A record of the independent verification will be maintained.

Should the University have a doubt over provider’s credentials, then the University’s Merchant Bank will be contacted and those concerns will be raised.

3.2. **Assessment of card data processing requirements and implementation of acceptable working practices**

Schools or Units must not implement business processes that involve the processing of card data without first consulting with the Finance Operations Manager, who will advise on how data are to be processed.

3.3. **Internal audit and review (compliance with this policy)**

The University will regularly (at least once within a period of 24 months) undertake an audit/review of all card data operations: to understand if they are consistent with the objectives of this policy. Should card data be processed outwith policy requirements, then the Finance Operations Manager will make recommendations on what changes are required.

3.4. **PCI DSS certification: in-house processing of card data**

Finance, with the support of IT Services will make returns on PCI DSS compliance to the University’s Merchant Bank or their appointee when required.
3.5. **Training**

Finance and IT Services as appropriate will provide general training on the secure use of card data and an overview of the University’s requirement to adhere to the PCI DSS standard as part of general training and awareness on information and data security.

4. **Responsibilities**

4.1. **Finance**
- Verifying the credentials/certification and maintaining records of whether a third party provider has or does not have the necessary qualification to provide level 1 PCI DSS processing services;
- Promoting the policy and its implementation across the University;
- Providing training and awareness;
- Working with Schools and Services to assess levels of compliance and to provide support to address any gaps.

4.2. **IT Services**
- Providing technical guidance necessary to assess and implement card processing solutions that are PCI DSS compliant;
- To provide the necessary technical support to support the implementation of this policy; and
- Provide necessary information governance support in this area.

4.3. **Heads of School/Units and card data business process owners**
- Ensuring that their School or Unit achieves compliance with this policy;
- Where there are gaps in the implementation of the policy that these are brought to the attention of Finance; and
- To work with Finance and/or IT Services to implement any measures required to secure compliance with this policy.

5. **Review**

This policy will be reviewed at regular intervals. The review period will be approved by the University ICT Strategy and Planning Group and recorded on the accompanying coversheet. Any significant change to the PCI DSS standard or University Policy or procedures primarily concerned with information confidentiality, integrity and accessibility may trigger an earlier review. This policy will be presented to the University ICT Strategy and Planning Group for approval.

6. **Policy breaches**

6.1. **Failure to process card data in a manner that is PCI DSS compliant**

In the first instance any suspicion of a breach of this policy should be reported to Finance Operations Manager. A serious breach of this policy will be reported to the Director of Finance.

The Finance Operations Manager may then advise if card data processing can continue without change, continue subject to the implementation of agreed actions, or if processing has to be suspended with immediate effect.
7. Sanctions

Failure to comply with this policy can introduce a range of threats to students, staff, external customers and the University, including the possibility that the University would breach the requirements of our banks, which require that we maintain compliance with the PCI DSS standard in respect to card data processing.

Where it is found that this policy has been breached, this will be considered at a local level between the line manager and the member of staff etc. with the necessary input from Finance and/or IT Services. It is anticipated that in most instances, guidance and/or training will help to resolve any problems. In significant and/or repeated cases, it may be appropriate for the line manager to follow existing capability frameworks to resolve issues.

Failure to resolve issues may involve the suspension of card processing. Should a serious breach occur it may be appropriate for action to be taken under the University’s disciplinary procedures (as applicable).

Where contractual terms have been broken the University will review its position with that party. This could lead to termination of a contract of employment, studies, research or the provision of goods/services. Where it is believed that a criminal action has occurred, the University will also report this to law enforcement agencies. The University also reserves the right to pursue through the Courts a breach of the common law of confidence where it believes that such action is justified. This may also include the pursuit of civil damages against any third party. The University will also advise third parties of any infringements of their rights.

8. Availability

This Policy will be published on the University Website. The policy can be made available in different formats, please direct any requests to the Associate Chief Information Officer (Information Assurance & Governance).

9. Contacts/further information

Enquiries regarding this policy can in the first instance be directed to the University Finance Operations Manager.