Payment Card Industry - Data Security Standard (PCI DSS) v3.2
Incident Response
# Version and Ownership

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.01</td>
<td>26/10/2016</td>
<td>Chris Willis</td>
<td>Initial Document creation - PCI DSS v3.2</td>
</tr>
<tr>
<td>0.02</td>
<td>20/01/2017</td>
<td>Chris Willis, Sinead O’Brien &amp; Tom Griffin</td>
<td>First draft finalised</td>
</tr>
<tr>
<td>0.02</td>
<td>10/02/2017</td>
<td>Chris Willis, Sinead O’Brien &amp; Tom Griffin</td>
<td>Version 0.02 approved by CiCS Exec.</td>
</tr>
<tr>
<td>0.03</td>
<td>24/04/2017</td>
<td>Chris Willis, Sinead O’Brien &amp; Tom Griffin</td>
<td>Updated to reflect that not all security events need escalating 24/7</td>
</tr>
<tr>
<td>0.03</td>
<td>12/05/2017</td>
<td>Chris Willis, Sinead O’Brien &amp; Tom Griffin</td>
<td>Version 0.03 approved by CiCS Exec.</td>
</tr>
<tr>
<td>1.0</td>
<td>31/10/2017</td>
<td>Chris Willis, Sinead O’Brien &amp; Tom Griffin</td>
<td>Version 1.0 approved by CiCS Exec</td>
</tr>
<tr>
<td>1.1</td>
<td>30/01/2018</td>
<td>Chris Willis, Tom Griffin &amp; Sinead O’Brien</td>
<td>Updated to include references to the University’s Major Incident Plan. Version 1.1 approved by CiCS Exec.</td>
</tr>
<tr>
<td>1.2</td>
<td>17/04/2018</td>
<td>Chris Willis, Tom Griffin &amp; Sinead O’Brien</td>
<td>Responsibilities section added and finance operational leads updated following recent staff changes.</td>
</tr>
<tr>
<td>1.3</td>
<td>01/05/2018</td>
<td>Sinead O’Brien, Chris Willis &amp; Tom Griffin</td>
<td>Remove requirements that are no longer applicable due to reduction in CDE scope.</td>
</tr>
<tr>
<td>1.4</td>
<td>08/11/2018</td>
<td>Helen Coffey, Sarah Turner</td>
<td>Updated PCI Response Team</td>
</tr>
</tbody>
</table>
# Table of Contents

## Introduction 4

## Incident Response - General Principles 5

## Incident Response - The 6 PCI DSS Incident Management Steps 5

1. Preparation 5
2. Identification 6
3. Containment 10
4. Investigation 10
5. Recovery 12
6. Review 12

## Glossary of terms 13

## Appendix A - Reporting Timeline 14

## Appendix B - PCI Response Team 16

- Incident Controllers 16
- Finance Senior Management 16
- Finance Operational Leads 16
- CiCS Senior Management 16
- CiCS Operational Leads 16
- Supporting Staff 17

## Appendix D - Worldpay Incident Reporting 18

## Appendix E - Service Providers 19

## Appendix F - Card Brands 20

## Appendix H - Misc Other Professional Agencies 21

## Appendix J - Template for Incident Log 22
Introduction

This document presents the Incident Response Plan should any card data related incident occur. This document is designed to support The University of Sheffield’s implementation of the Payment Card Industry Data Security Standard (PCI DSS) compliance version 3.2, in relation to any incident occurring within the cardholder environment. An incident is described as any violation of policy, law, or unacceptable act that involves information assets, such as computers, networks, smartphones, etc.

- Staff in the context of this document refers to all individuals employed by the University of Sheffield or its subsidiaries or paid by the University of Sheffield or its subsidiaries to perform duties that require the individual to store, process or transmit card information.
- We adhere to the PCI DSS and all staff in the CDE must be aware of The University Of Sheffield PCI DSS Information Security Policy.
- The University of Sheffield use SANS as our overarching process for response; preparation, identification, containment, investigation, recovery and review.
- The University of Sheffield escalate in accordance with the Information Security Incident Policy and Procedure.
- An Account Data Compromise (ADC) is an intrusion into computer system(s) or access to physical cardholder data where unauthorised disclosure, modification, or destruction of cardholder data is suspected. The University’s Major Incident Plan should also be taken into consideration when responding to any ADC.
- The incident response plan covered in the document supports version 3.2 of the PCI DSS.
- It is required that this plan is reviewed and tested at least annually (PCI DSS 12.10.2). As part of this annual review the Incident Response plan will be modified and evolved to incorporate industry developments.(PCI DSS 12.10.6)
- This document currently outlines the University’s commitment to meet the following PCI DSS requirements:

### Requirement 12: Maintain a policy that addresses information security for all personnel

<table>
<thead>
<tr>
<th>12.10</th>
<th>Implement an incident response plan. Be prepared to respond immediately to a system breach.</th>
</tr>
</thead>
</table>
| 12.10.1 | Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: 
- Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum
- Specific incident response procedures
- Business recovery and continuity procedures
- Data backup processes
- Analysis of legal requirements for reporting compromises
- Coverage and responses of all critical system components
- Reference or inclusion of incident response procedures from the payment brands |
| 12.10.2 | Review and test the plan, including all elements listed in Requirement 12.10.1, at least annually. |
| 12.10.6 | Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. |
Incident Response - General Principles

The University’s approach to PCI DSS Incident Management comprises of six steps:

1. Preparation
2. Identification
3. Containment
4. Investigation
5. Recovery
6. Review

Responsibilities

Responsibilities for all personnel responding to an incident and those with an incident management role within the University’s cardholder data environment (CDE) are covered within this document.

Incident Response - The 6 PCI DSS Incident Management Steps

1. Preparation

The following key elements have been implemented in order to help mitigate against any potential problems that may hinder our ability to handle an incident.

1.1 PCI DSS Incident Response

The University of Sheffield will maintain this document as a PCI DSS incident response plan. This incident response plan has been prepared as the guide to follow in the event of a card related incident. It is required that this plan is reviewed and tested at least annually. Please take particular note of the timeline detailed in Appendix A. This lists various external contacts that The University is required to inform in the case of a payment card incident.

1.2 PCI response team

See Appendix B for contact information for the PCI Response Team. See Appendices D-H for contact information for various external bodies that may need to be involved in the incident response. All members of the PCI Response Team will have received training in the PCI DSS. The team will be familiar with the University’s CDE, its components and network, and will be capable of being convened at very short notice.

1.3 Staff associated with CDE

Appendix B contains contact information on various internal staff related to the CDE.

1.4 Communications Plan

Internal communication are to be managed by the incident controller as listed in Appendix B. Any communications with the general public will be handled by the communications manager as listed in Appendix B. All communications with the acquirer, card brands, service providers, law enforcement and the public will be coordinated by the Incident Management Team.
1.5 Logging
If a security event, potential incident or actual incident is identified then every action taken must be documented (e.g. decisions made, information gathered, commands typed, systems affected, etc). A template Incident Log is available in Appendix J. This Incident Log should be able to answer the Who, What, When, Where, Why, and How questions should they ever arise.

1.6 Documentation
Links to important PCI DSS informational documents are available in the table below. These documents will be kept up to date by the people listed in the PCI BAU document

<table>
<thead>
<tr>
<th>Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network diagram</td>
</tr>
<tr>
<td>Asset Register</td>
</tr>
<tr>
<td>Firewall Rules</td>
</tr>
<tr>
<td>PCI DSS Policies</td>
</tr>
<tr>
<td>PCI DSS Network Configuration</td>
</tr>
</tbody>
</table>

1.7 Information Sources
If available then the following information sources (e.g. logs, alerts, records, changes) will be kept for both internal and external investigators to review:
- CCTV recordings
- CDE system logs (e.g. antivirus, firewall, security event)
- Alerts (e.g. FIM, firewall, network)
- Change Management records
- Access Control logs (both physical and logical)

1.8 Alerts
Alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems will be received in real time and must be investigated on receipt. Any alerts which are generated out of hours must be investigated at the first opportunity in accordance with the Operational Security Standard. (PCI DSS 12.10.5)

1.9 Training
Training will be given to staff as appropriate. This includes:
- Members of the PCI Response Team will be briefed on their expected roles.
- Incident Controllers will receive incident management training.
- Senior Management in CiCS and Finance will be briefed on this process.
- The CiCS Helpdesk and University Control will be briefed on their role in Incident Response and made aware of escalation routes
- All staff working with cardholder data on behalf of University will be made aware of this policy.

2. Identification
The following steps outline how a security event is identified as a potential incident, assessed and then, if necessary, identified as an actual incident warranting further investigation.
2.1 Potential incident identified
Identification and escalation table

<table>
<thead>
<tr>
<th>Event</th>
<th>Escalate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Found card - A member of staff finds a credit/debit card or a wallet.</td>
<td>Follow the UoS PCI DSS Found card policy in the <a href="#">PCI DSS Finance standard</a>. No further action required by the reporter of the security event.</td>
</tr>
<tr>
<td>Small amounts of unsolicited cardholder data - A member of staff receives data relating to less than 5 payment cards. The member of staff must not have asked for the cardholder data.</td>
<td>Email <a href="mailto:pcidss@sheffield.ac.uk">pcidss@sheffield.ac.uk</a>. DO NOT forward the email or a copy of the file in question. The reporter will be contacted by the PCI DSS incident response team who will advise on further action required.</td>
</tr>
<tr>
<td>All security events involving cardholder data or systems that can impact on the security of cardholder data, not covered above, must be considered as potential incidents.</td>
<td>Anyone discovering or being informed of a potential incident should <strong>immediately</strong> report the potential incident by phone (do not leave voicemail or send email) to the CiCS Helpdesk on 0114 222 1111. If the incident occurs outside of normal working hours then contact University Security on 0114 222 4085.</td>
</tr>
</tbody>
</table>

A security event is defined as:

“A security event is an occurrence considered by an organization to have potential security implications to a system or its environment. In the context of PCI DSS, security events identify suspicious or anomalous activity.”

Examples include, but are not limited to, the following:

- A report of a failure to follow policy or process
- Evidence, or suspicion, of tampering with a device within the CDE
- A security alert from a system within the CDE
- An external report of an incident, for example from a 3rd party such as WPM, Worldpay, MCR, Verifone, Rocco Creative, Ex Libris, Student Pad, etc.
- Theft of payment card equipment
- Receipt of an email containing cardholder data for 5 or more cards where no member of staff has requested that the cardholder data be sent by email.
- Discovery of a file on University servers containing cardholder data for 5 or more cards.

2.2 Potential Incident Reporting
Anyone discovering or being informed of a security event (not covered by the events above) must **immediately** report the potential incident by phone (do not leave voicemail or send email).
email) to the CiCS Helpdesk on 0114 222 1111. If the incident occurs outside of normal working hours then contact University Security on 0114 222 4085.

The potential incident will be managed in accordance with the University’s Information Security Incident Policy and Process.

2.3 Actions to be taken

In the case of suspected exposure of payment card cardholder information:

- DO NOT attempt to process any further payment through the payment system. The payment system can be a terminal, pin pad, EPOS, PED, computer, application (e.g. DataDivider, WPM) or any other electronic payment device.
- DO NOT shut down the suspected machine. DO NOT disconnect the power cable.
- DO disconnect the physical network cable from the network jack and/or telephone socket at the back of the machine immediately.
- DO NOT alter or access the machine using either privileged or nonprivileged accounts (including as ROOT or remotely).
- If already logged in during the suspected compromise DO NOT log out, DO NOT open any more files or any additional software services.
- DO document all steps taken. Include the: date, time, location, action taken, reason for the action, person(s) involved and anyone informed for each action taken.
- DO physically label the machine to not be touched by anyone except as directed by the Incident Management Team.
- DO keep any suspected machine under supervision until further information is given by the Incident Management Team.
- Anticipate that the Incident Management Team, as part of the incident response, will collect all logs including remote logs and ancillary electronic evidence. Therefore it is important to preserve the current state of systems; files and data must not be modified or deleted.
- If the device is a Verifone P2PE PED and there is any evidence/suspicion of tampering then the device must be removed from service immediately. We will then investigate in accordance with the relevant PIM and any University processes.
- If the device is a Worldpay PED and there is any evidence/suspicion of tampering; place the PED in a safe bag/box so that evidence is protected and ready to be handed to the authorities or specialist investigators.

2.4 Potential Incident Logging

The potential incident will be passed to an Incident Controller (see Appendix B for a list of Incident Controllers and deputies).

The Incident Controller will own the potential incident. The Incident Controller will log the potential incident in the Incidents Spreadsheet.

2.5 Potential Incident Assessment

The Incident Controller will assess the potential incident. Where necessary they will pull together relevant personnel to help with the assessment.

---

1 University Information Security Incident Policy - [http://www.shef.ac.uk/cics/policies/securityincident](http://www.shef.ac.uk/cics/policies/securityincident)
If the security event is not deemed to be an incident then the potential incident will be closed. The assessment and decision making processes must be recorded in the Incidents Spreadsheet.

If it is found that there is an actual incident then an Incident Management Team will be formed in accordance with the University Information Security Policy. The assessment and decision making processes must be recorded in the Incidents Spreadsheet.
3. Containment

3.1 Incident initiation

The Incident will be managed in accordance with the University Information Security Policy and Process.

An Incident Management Team will be formed with relevant staff from the PCI Response Team (Appendix B) and any other appropriate staff.

A senior member of CiCS/Finance staff will be identified as the Incident Manager and they will oversee the incident. The Incident Controller (Appendix B) will provide support and expertise to assist the Incident Manager.

An individual Incident Log will be opened (Appendix J) and the spreadsheet will be updated. The Incident Log will be maintained by the Incident Controller.

Communication and coordination between members of the Incident Management Team (and management) is critical, especially if the scope of the incident can have a significant impact on business operations.

3.2 Incident Containment

The Incident Management Team should review actions taken to date and consider if any further containment activities should take place. These should be in accordance with the principles outlined in “2.3 Actions to be taken”.

3.3 Preservation of Evidence and Incident Logs

All incident responders must document everything they are doing. All logs and electronic evidence must be preserved and a full record must be maintained of all action taken. A template Incident Log is available in Appendix J.

4. Investigation

4.1 Internal Reporting

Depending on the nature and potential severity of the breach the Incident Management Team may contact the following:

- Senior Management - Finance
- Senior Management - CiCS
- Technical staff supporting the affected CDE components
- Finance staff supporting the affected payment channels
- Business units using the affected payment channels
- Communications staff - e.g. CICS communications team, University communications team
- University Security
- Other members of the PCI Response Team as appropriate
- PCI DSS Steering Group

4.2 External and Internal Reporting

The Incident Management Team will be responsible for determining if the acquirer needs to be notified of a suspected breach. In the event of a breach, or a suspected breach the
University’s Acquirer must be notified with 24 hours. Contact details for the Acquirer are listed under **Appendix D**.

Who needs to be notified in addition to this will depend on which payment channel(s) are believed to have been compromised.

- **Ecommerce server:**
  - Income Office Management Team
  - Related Service Providers including WPM
  - External company/internal CiCS team responsible for website(s).

- **Worldpay Standalone PEDs:**
  - Income Office Management Team

- **MCR Till with integrated Verifone PEDs:**
  - Income Office Management Team
  - ACS/UNICUS Management Team
  - Verifone must be notified immediately of compromised P2PE devices
  - MCR Service Providers

- **Computers that card numbers are typed into (e.g. Datadivider enabled PCs):**
  - Income Office Management Team
  - Related Service Providers

Reporting details for external companies can be found in **Appendices D-H** at the bottom of this document.

### 4.3 Onward reporting to Acquirer and card brands

The University will take guidance from our Acquirer in terms of onward reporting to the card brands. In the event that a suspected breach is uncovered out of hours and the University Acquirer is unavailable to assist, then the Incident Management Team will make the decision as to whether the breach is significant enough to warrant reporting to Visa and Mastercard directly. Contact details for the card brands are listed below in **Appendix F**.

### 4.4 PFI Companies

Depending on the scale of the breach it may be necessary to engage a PCI Forensic Investigation company. A list of companies registered as approved PFIs with the PCI SSC are available here: [https://www.pcisecuritystandards.org/assessors_and_solutions/pci_forensic_investigators](https://www.pcisecuritystandards.org/assessors_and_solutions/pci_forensic_investigators). If the use of a PFI is required please take special note of the timeline that must be adhered to for their engagement and investigation. See **Appendix A**. Visa Europe advise that on average a Full PFI Investigation can take from 6-12 weeks to complete and once complete there is a requirement for the merchant to become PCI DSS compliant to Level 1.

### 4.5 Police - Action Fraud

Action Fraud is the UK’s national reporting centre for fraud and cybercrime, and takes crime and information reports on behalf of the police and gives advice and fraud prevention guidance. Action Fraud must be notified within 24 hours of a breach. Communication with the Police should be initiated by the University security “Control Room”. Action Fraud does not have investigative powers, however, the reports taken by Action Fraud are sent to the National Fraud Intelligence Bureau (NFIB) which is run by the City of London Police, the national lead force for fraud. The NFIB collates and analyses intelligence on fraud, identifying viable lines of enquiry and developing packages for submitting to a police force for investigation.
Contact with this agency or any other agency must be recorded in the Incident Log (Appendix J).

4.6 FFA UK
Financial Fraud Action UK provides general information and advice on the prevention of payment fraud. They do not offer any investigation or law enforcement related services. Contact with this agency must be recorded in the Incident Log (Appendix J).

4.7 University Corporate Communications
Corporate Communications is responsible for ensuring a consistent marketing and communications focus across the University. They are also responsible for managing public communications around an incident of this nature.
http://www.sheffield.ac.uk/corporate-communications

4.8 Further Reporting to payment card brands
The card brands will require a list/upload of card details for all cards that have potentially been compromised, details of the breach, the University’s PCI DSS status at the time of the breach, information from any PFI’s that occur, any efforts made to correct the situation, that the University is no longer compromised and proof that the University has successfully achieved compliance validated by an outside QSA.

4.9 Information Commissioner’s Office
The ICO is the UK’s independent body set up to uphold information rights. Cardholder data is considered to be personal data, as such if it has been lost during the breach The University is required to report this loss to the Information Commissioner’s Office.

5. Recovery
Recovery operations will be based on the conclusions of the PFI investigation and/or on the advice of the University’s Acquirer. Work required for this phase will be based upon the full circumstances of the breach and if a breach involving the University’s CDE was proven to have taken place. Recovery operations will also be influenced by the defined status of the University’s PCI-DSS compliance at the time the incident took place.

Prior to resuming payment card operations using CDE components associated with a breach (on conclusion of the PFI investigation, if one has taken place), the re-build, configuration, software installation, network connectivity, etc. of the CDE, as appropriate, will be independently validated by a PCI-DSS QSA. An up to date list of PCI-DSS certified PCI-DSS QSAs can be found on the PCI SSC website at https://www.pcisecuritystandards.org/approved_companies_providers/qsa_companies.php

6. Review
In addition to dealing with each incident in line with this incident response plan, each potential/actual incident will be reviewed by the University’s PCI DSS Steering Group on a quarterly basis.

Once the University has recovered from the incident, the Incident Management Team and all affected parties will meet to review its security strategy, Incident Response Plan, response time and PCI DSS processes. An analysis will be made of how the incident was detected, notified, handled and contained and the Incident Response Plan will be modified and evolved accordingly. (PCI DSS 12.10.6)
### Glossary of terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADC</td>
<td>Account Data Compromise</td>
</tr>
<tr>
<td>BAU</td>
<td>Business As Usual</td>
</tr>
<tr>
<td>CDE</td>
<td>Cardholder data environment</td>
</tr>
<tr>
<td>CHD</td>
<td>Cardholder data</td>
</tr>
<tr>
<td>PAN</td>
<td>Primary account number</td>
</tr>
<tr>
<td>PCI DSS</td>
<td>Payment Card Industry Data Security Standard</td>
</tr>
<tr>
<td>PCI SSC</td>
<td>Payment Card Industry Security Standards Council</td>
</tr>
<tr>
<td>PED</td>
<td>Pin entry device</td>
</tr>
<tr>
<td>PFI</td>
<td>PCI Forensic Investigators</td>
</tr>
<tr>
<td>SAD</td>
<td>Secure authentication data</td>
</tr>
</tbody>
</table>
Appendix A - Reporting Timeline

The reporting schedule is mandated by the card brands (Visa\textsuperscript{2} and Mastercard\textsuperscript{3}). This timeline may vary between brands. Where possible the applicable card brand has been included, however it is best to refer to the card brands separate incident documents to get their up to date incident reporting timelines.

- Immediately (Within 24 hours):
  - Notify the University’s Acquirer.
  - Notify all affected payment brands (either directly or through Acquirer)
  - Notify the Police - Action Fraud Agency
  - Provide as much information as possible about the breach. (Mastercard)
  - Provide the card brands card details associated with the incident. (Mastercard)

- Within 48 hours of notification:
  - Provide Visa with status of compliance with PCI DSS and, if applicable, PCI Payment Application Data Security Standard (PA-DSS) and PCI PIN security requirements at the time of the incident.

- Within 72 hours of notification:
  - Provide Visa Initial Investigation Report, either to the acquiring bank or directly to Visa. The form for this is available on page 4 of the Visa “What to do if compromised” document: https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf
  - Engage the services of a PCI SSC Forensic Investigator (PFI) (Mastercard). The PFI engaged to conduct the investigation must not have provided the last PCI compliance report concerning the system or environment to be examined. The card brand may engage a PFI directly on behalf of the merchant. The Customer on whose behalf the PFI is so engaged will be responsible for all costs associated with the investigation.
  - Consider the requirement to report serious breaches to the ICO. Any decision made to report, or not, should be recorded in the Incident Log.

- Within five (5) business days of notification:
  - Ensure that the PFI is engaged (or the contract is signed) (Visa).
  - Identify to Mastercard the engaged PFI and confirm that such PFI has commenced its investigation. (Mastercard)
  - Provide All Exposed Accounts to Visa.

- Within eight (8) business days from notification:
  - Ensure that the PFI submits to Mastercard a preliminary forensic report detailing all investigative findings to date.

- Within ten (10) business days from when the PFI is engaged (or the contract is signed):
  - Ensure initial work is underway and provide the initial forensic (i.e., preliminary) report to Visa.

- Within twenty (20) business days from the commencement of the forensic investigation:
  - Provide to Mastercard a final forensic report. (Mastercard)

- Within ten (10) business days of completion of the forensic review:

\textsuperscript{2} Visa “What To Do If Compromised” https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf
- Provide a final forensic report to Visa. 
  As soon as practical, but no later than 60 calendar days from the conclusion of the forensics evaluation, the compromised entity or its Acquirer must provide evidence from a QSA and an ASV that the compromised entity has achieved full compliance with the Payment Card Industry Data Security Standard (Mastercard).
Appendix B - PCI Response Team

Incident Controllers

<table>
<thead>
<tr>
<th>Name</th>
<th>Contact</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chris Willis</td>
<td>Incident Contacts have out of hours contact details</td>
<td>Incident Controller - ISA &amp; Information Security Manager</td>
</tr>
<tr>
<td>Tom Griffin</td>
<td>Incident Contacts have out of hours contact details</td>
<td>Deputy Incident Controller - Network and Security Specialist</td>
</tr>
<tr>
<td>Sarah Turner</td>
<td>Incident Contacts have out of hours contact details</td>
<td>Income Manager</td>
</tr>
</tbody>
</table>

Finance Senior Management

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Helen Dingle</td>
<td>Chief Financial Officer</td>
</tr>
<tr>
<td>Victoria Jackson</td>
<td>Director of Finance</td>
</tr>
<tr>
<td>Robert Hebblethwaite</td>
<td>Assistant Director - Financial Services</td>
</tr>
</tbody>
</table>

Finance Operational Leads

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sarah Turner</td>
<td>Income Manager</td>
</tr>
<tr>
<td>Helen Coffey</td>
<td>Senior Financial Services Assistant</td>
</tr>
<tr>
<td>Daniel Rhodes</td>
<td>Financial Services Assistant</td>
</tr>
</tbody>
</table>

CiCS Senior Management

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>John McAuley</td>
<td>Director of CiCS</td>
</tr>
<tr>
<td>Nathan Cunningham</td>
<td>Assistant Director</td>
</tr>
<tr>
<td>David Surtees</td>
<td>Assistant Director</td>
</tr>
<tr>
<td>Katherine Winter</td>
<td>Assistant Director</td>
</tr>
</tbody>
</table>

CiCS Operational Leads

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chris Willis</td>
<td>Head of Information Security</td>
</tr>
<tr>
<td>Tom Griffin</td>
<td>IT Security Manager</td>
</tr>
<tr>
<td>Mike Greenwood</td>
<td>Data Network Manager</td>
</tr>
<tr>
<td>Anne Rodgers</td>
<td>Head of Corporate Information</td>
</tr>
<tr>
<td>Razia Ali</td>
<td>ICT Support Co-ordinator</td>
</tr>
</tbody>
</table>
## Supporting Staff

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracey Garner</td>
<td>ACS/Unicus - PED machines, GeniUS Online Pathway</td>
</tr>
<tr>
<td>Steve Bulley</td>
<td>Accommodation/Starrez</td>
</tr>
<tr>
<td>Lee Beckett</td>
<td>Sports Sheffield - PED machines, Sports Online Pathway</td>
</tr>
<tr>
<td>Rob Davies/Chris Clow</td>
<td>Print Credits Online Pathway</td>
</tr>
<tr>
<td>Jayne Conboye</td>
<td>Student Pad Online Pathway (LandLord)</td>
</tr>
<tr>
<td>Steven Sharples</td>
<td>Xerox Online Pathway</td>
</tr>
<tr>
<td>Steve Clarke</td>
<td>Finance and Stewardship Co-ordinator</td>
</tr>
<tr>
<td>Tracey Garner</td>
<td>Finance Manager for ACS and UNICUS</td>
</tr>
<tr>
<td>Kate Godber</td>
<td>Head of Finance - Students’ Union</td>
</tr>
<tr>
<td>David Orwin</td>
<td>Head of Finance (ACS &amp; UNICUS)</td>
</tr>
<tr>
<td>Tony Sweeney</td>
<td>Head of Technology Development - Students’ Union</td>
</tr>
</tbody>
</table>
Appendix D - Worldpay Incident Reporting

In the event of an incident contact **both** Danny Gunter and the payment data security mailbox. They will pass the account and any initial information to the ADC team in Worldpay.

<table>
<thead>
<tr>
<th>Name</th>
<th>Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Danny Gunter</td>
<td>Franchise Development &amp; Management</td>
</tr>
<tr>
<td></td>
<td>Payment Data Security Consultant</td>
</tr>
<tr>
<td></td>
<td>T: +44 (0) 203 664 4351</td>
</tr>
<tr>
<td></td>
<td>The Walbrook Building</td>
</tr>
<tr>
<td></td>
<td>London</td>
</tr>
<tr>
<td>Payment data security mailbox</td>
<td><a href="mailto:rscpaymentdatasecurity@worldpay.com">rscpaymentdatasecurity@worldpay.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:payment_datasecurity@worldpay.com">payment_datasecurity@worldpay.com</a></td>
</tr>
</tbody>
</table>
### Appendix E - Service Providers

<table>
<thead>
<tr>
<th>Name</th>
<th>Contact</th>
</tr>
</thead>
</table>
| WPM Education          | 26 Victoria Way  
Burgess Hill  
West Sussex  
RH15 9NF  
0844 264 1580          |
| DataDivider            | Graham Thompson  
gthompson@datadivider.com  
Sales and Marketing Director  
DataDivider  
6472 Camden Ave, Suite 102B,  
San Jose, CA 95120, US  
US Cell: +1 669 225 6250  
UK Mobile: +44 7944 860188  
Skype: grahamwthompson  
Corporate US Phone: (408) 457-0216  
Corporate US Fax: (650) 276 7336  
Website: [www.datadivider.com](http://www.datadivider.com)  
Support Email: DataDivider_Support@datadivider.com |
| MCR Systems            | Technical: support@mcr-systems.co.uk (0116 299 7007)  
Escalation: Technical Support Manager: John.Lakin@mcr-systems.co.uk  
0116 299 7000 Operations Director: Leigh.McManus@mcr-systems.co.uk  
0116 299 7000 |
| Verifone UK Ltd        | Verifone Services UK, 100 Eureka Park, Ashford, Kent, TN25 4AZ  
Main Telephone Number: 08444 828200  
Main Fax: 08444 828210  
Merchant Helpdesk Telephone: 08444 828222  
Merchant Helpdesk Fax: 08444 828223  
Technical Services: 08444 828273  
Customer Services: 08444 828268  
Sales Enquiries ocius.enquiries@verifone.com  
Merchant Helpdesk ocius.helpdesk@verifone.com  
Technical Services ocius.techservices@verifone.com  
Customer Services ocius.customer.services@verifone.com  
Website: [www.verifone.co.uk](http://www.verifone.co.uk) |
## Appendix F - Card Brands

<table>
<thead>
<tr>
<th>Name</th>
<th>Contact</th>
</tr>
</thead>
</table>
| Visa Europe | Visa Europe Data Compromise Team Manager  
Telephone: 0207 795 5031  
Email: datacompromise@visa.com |

For Visa’s guidelines on what to do if compromised please see  

| MasterCard | For reporting requirements to MasterCard please see  

| AMEX | For reporting requirements for American Express please see  
https://www.americanexpress.com/in/content/merchant/support/data-security/merchant-information.html |

| Discover | For reporting requirements for Discover please see  

| JCB | For reporting requirements for JCB please visit  
https://www.jcbusa.com |
### Appendix H - Misc Other Professional Agencies

<table>
<thead>
<tr>
<th>Name</th>
<th>Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Crime Agency</td>
<td>24 hour reporting. Telephone: 0370 496 7622 and ask for National Cybercrime Unit Duty Officer</td>
</tr>
<tr>
<td>Financial Fraud Action (FFA UK)</td>
<td>Financial Fraud Action UK provides general information and advice on the prevention of payment fraud. They do not offer any investigation or law enforcement related services. <a href="https://www.financialfraudaction.org.uk/">https://www.financialfraudaction.org.uk/</a> Telephone: 020 3217 8436</td>
</tr>
<tr>
<td>Information Commissioner’s Office (ICO)</td>
<td>Report a breach <a href="https://ico.org.uk/for-organisations/report-a-breach/">https://ico.org.uk/for-organisations/report-a-breach/</a> Data has been unlawfully obtained or accessed (a breach of section 55 of the Data Protection Act) - Will need reporting to the ICO.</td>
</tr>
</tbody>
</table>
### Appendix J - Template for Incident Log

<table>
<thead>
<tr>
<th>Action date &amp; time</th>
<th>Details of action taken</th>
<th>Person who took this action</th>
<th>Who else was present</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>