Cardholder Data Security Rules & Processes

Owners: Bridget Midwinter (Chief Cashier)
Jonathan Ashton (Head of Security Governance Risk and Compliance)

1 Definitions ........................................................................................................................................... 2
2 Cardholder Data security rules ............................................................................................................ 2
  2.1 Introduction to the Rules ............................................................................................................... 2
  2.2 Locations authorised to handle Cardholder Data ......................................................................... 2
  2.3 Handling of Cardholder Data ..................................................................................................... 3
  2.4 Access to Cardholder Data .......................................................................................................... 5
3 Cardholder Data Security Processes ................................................................................................. 7
  3.1 Introduction to the Card handling Processes .............................................................................. 7
  3.2 Methods of obtaining Cardholder Data .................................................................................... 7
  3.3 Transferring Cardholder Data to Other Units or Teams ............................................................. 9
  3.4 Storing Cardholder Data ............................................................................................................. 9
  3.5 Controlling Access to Card Holder Data .................................................................................... 10
  3.6 Reporting Incidents Involving Cardholder Data ....................................................................... 10
  3.7 Compliance with PCI & University Rules ................................................................................... 11
4 Approved Suppliers and Solutions ..................................................................................................... 13
  4.1 Ecommerce ............................................................................................................................... 13
  4.2 Face to Face ............................................................................................................................. 13
1 DEFINITIONS

Cardholder Data: At a minimum, Cardholder Data consists of the full PAN. Cardholder Data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code.

PAN: Acronym for “primary account number” and also referred to as “account number.” Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.

Sensitive Authentication Data: Security-related information used to authenticate cardholders and/or authorize payment card transactions. This includes, but is not limited to, card validation codes/values (sometimes known as CVV, CAV2, CVC2, CVV2 or CID), full track data (from the magnetic stripe or equivalent on a chip), PINs, and PIN blocks.

Unit or Units: A Department, Faculty or central division of the Collegiate University.

2 CARDHOLDER DATA SECURITY RULES

2.1 INTRODUCTION TO THE RULES

These rules state the requirements for handling Cardholder Data in an authorised manner, and constitute the conditions of use that units wishing to take card payments must sign up to in order to be established as an authorised University merchant.

Heads of Department and Faculty board chairs are responsible for the security of Cardholder Data and compliance with applicable PCI-DSS requirements. As such they must be familiar with and understand their responsibilities and requirements for securing Cardholder Data including:

- these rules;
- University Cardholder Data Security Policy; and
- The University’s baseline requirements for information and IT security.

Cardholder Data has been classified as “Confidential” by the Finance Division under the University’s classification scheme. The following rules describe where, how and by whom Cardholder Data may be processed as authorised by the Finance Division.

2.2 LOCATIONS AUTHORISED TO HANDLE CARDHOLDER DATA

2.2.1 Cardholder Data may only be processed in, or transmitted from, specifically authorised locations within the University and/or authorised third-parties.

In order to be authorised, units must, as a minimum:

- Obtain authorisation from the Finance Division and sign up to these handling rules prior to processing or transmitting Cardholder Data on behalf of the University, including when employing a third party to store, process or transmit card details on behalf of the University;
- Maintain up-to-date records of all local requirements for complying with PCI-DSS;

1 https://infosec.ox.ac.uk/sites/default/files/Information%20Classification%20Scheme.pdf
Cardholder Data Security
Rules & Processes
Version 2.0

• Nominate a dedicated point of contact for all matters relating to PCI compliance and security of Cardholder Data;
• Define local roles and responsibilities for maintaining compliance with the PCI-DSS and securing Cardholder Data;
• Carry out annual testing of compliance with all applicable PCI-DSS requirements in accordance with the specified PCI-DSS tests and submit annual self-assessments to the Finance Division to attest to compliance with those requirements; and
• Allow and respond to requests for audits (either remote or onsite) from the Finance Division, the Information Security Team, the Internal Auditors and/or any authorised third-party, to review and monitor processes in respect of handling Cardholder Data.

2.3 Handling of Cardholder Data

2.3.1 Cardholder Data must be used only for specific purposes which are explicitly approved by the Finance Division

These processes include transmission and/or processing of Cardholder Data for the purposes of:

• Face to face transactions using approved Pin Entry Devices (PEDs) and/or Electronic Point of Sale (EPOS) devices;
• Approved e-commerce channels; and
• Card not present transactions such as phone or web-based payments.

2.3.2 Cardholder Data may not be stored on any IT system or by any other electronic means.

2.3.3 Sensitive Authentication Data must never be written down or requested on a form.

2.3.4 Sensitive Authentication Data may not be stored or otherwise retained in any form after authorisation\(^2\) of cardholder transactions.

2.3.5 Cardholder Data must only be processed or transmitted using systems and technologies that are explicitly authorised and approved by the Finance Division; such systems include, but are not limited to, EPOS systems, Pin Entry Devices (PEDs), remote access technologies, wireless networks, laptops, tablets and removable media.

Finance Division will maintain an up-to-date list of all such devices in use across the Collegiate University, including any Terminal IDs and serial numbers, and the Finance Division must be advised of, and approve in advance, any changes to this environment in units, including the replacement of any devices.

Approved technologies and systems for processing Cardholder Data include:

• Approved Pin Entry Devices (PEDs) and/or Electronic Point of Sale (EPOS) devices which are:
  o Implemented as part of a validated P2PE solution;
  o Installed and configured in accordance with applicable PCI requirements by a suitably trained and qualified person; and

\(^2\) In the context of a payment card transaction, authorization occurs when a merchant receives transaction approval after the acquirer validates the transaction with the issuer/processor.
o Installed in an environment where all systems and system components within the Cardholder Data environment are compliant with applicable PCI-DSS requirements.

- Approved e-commerce channels include:
  o University sites where the entire payment page is received from, and returned to, an approved and authorised PCI-DSS compliant payment service provider (PSP) via a redirect process or iframe; and
  o Approved and authorised third-party maintained websites used to direct card payment via one of the methods described above.

The following technologies and systems are explicitly not approved:

- End user technologies such as email or social media; and
- E-commerce sites using direct posts, JavaScript created forms, APIs or any other method used to receive and return payments by directly processing Cardholder Data.

2.3.6 Cardholder Data must not be electronically scanned or sent using the University’s internal post.

2.3.7 All devices, systems and technologies used to process or transmit Cardholder Data must be installed and implemented in accordance with both the University’s baseline requirements for information and IT security and with applicable PCI-DSS requirements.

The baseline security requirements include, but are not limited to:

- Authentication to devices and technologies;
- Automatic disconnect of sessions for remote access technologies after a specific period of time; and
- Activation of remote-access technologies for vendors and business partners only when needed and deactivation after use.

2.3.8 Units must ensure that all devices are examined for evidence of tampering on a daily basis, and kept securely when not in use. Any concerns must be immediately reported, as per Section 3.6.

2.3.9 Laptops processing or transmitting Cardholder Data must have their drives fully encrypted via an approved, University-managed service.

2.3.10 Mobile Devices processing or transmitting Cardholder Data must comply with applicable PCI-DSS requirements.

At a minimum, devices must be:

- For a business purpose approved by the Cashiers Office;
- University managed;
- Protected by a PIN or passphrase;
- Configured in such a way that they can be remotely wiped;
- Encrypted;
- Configured to ensure they automatically lock after a period of inactivity (no more than 15 minutes);

---

3 [https://www.infosec.ox.ac.uk/guidance-policy/it-security](https://www.infosec.ox.ac.uk/guidance-policy/it-security)
2.3.11 Cardholder Data must only be processed or transmitted via University controlled and maintained devices.

2.3.12 Cardholder Data must be encrypted or otherwise secured when being transferred between internal or external systems.

2.3.13 All access to systems processing or transmitting Cardholder Data must be authenticated and audit trails kept for a minimum of 6 months.

2.3.14 Remote access to systems processing or transmitting Cardholder Data must be protected by two-factor authentication.

2.3.15 Physical copies of Cardholder Data must be explicitly approved, classified as confidential, handled in accordance with these handling rules and an audit trail maintained of all copies.

2.3.16 Physical copies of Cardholder Data must be labelled as such so that users/ recipients of Cardholder Data are explicitly aware of its classification and the intended audience.

2.3.17 Physical copies of Cardholder Data, held pending processing, must be kept in locked drawers, filing cabinets or the equivalent. Such data must be processed on the day of receipt, or in exceptional circumstances the next working day, before being destroyed.

2.3.18 Physical copies of Cardholder Data must be destroyed using a secure shredding service or a DIN level 3 or higher cross shredder when no longer required.

2.3.19 Physical copies of Cardholder Data must only be sent to the processing unit by hand, by special delivery or by secure cash carrier and a log of all sent items must be maintained.

2.3.20 Any suspected incident involving PCI data must be reported to cashiers@admin.ox.ac.uk within 4 working hours of discovery and on the same working day wherever possible.

2.3.21 Any suspected incident which involves potential compromise of information systems, such as EPOS tills or e-commerce sites, must be reported to local IT support and to oxcert@it.ox.ac.uk

2.4 ACCESS TO CARDHOLDER DATA

2.4.1 Cardholder Data must only be accessed by tightly restricted groups of explicitly authorised persons and in accordance with these handling rules.

Units processing Cardholder Data on behalf of the University must:

- Maintain a list of explicitly authorised staff who are involved with handling, and/or have access to, Cardholder Data;
- Ensure that any access to Cardholder Data is granted on a least privilege basis in accordance with job roles; and
Ensure that, as per the Baseline Requirements, each person accessing payment systems has an individual, non-shared user ID and password.

2.4.2 University users with privileged access to Cardholder Data or processes must be appropriately vetted and approved. See Section 3.5 for further details.

2.4.3 Cardholder Data must only be accessed by users who have been through appropriate training, and up to date training records must be maintained.

Units must ensure that all staff who are involved in handling Cardholder Data:

- Are aware that Cardholder Data is to be treated as confidential in accordance with the University’s classification scheme;
- Are aware of these handling rules, are reminded of, and sign to, them periodically and at least annually;
- Are subject to appropriate awareness training on at least an annual basis;
- Are trained to be aware of suspicious behaviour; and
- Have sufficient expertise to be able to advise Finance Division of local arrangements for storing, processing or transmitting Cardholder Data (including advising on technical arrangements and responding to technical queries e.g. when advising on potential weaknesses as identified by vulnerability scanning).

2.4.4 Third-party organisations processing Cardholder Data must be audited by an independent organisation and enter into a specific agreement with the University (including having signed up to the University's information security schedule).

Units must:

- Ensure that a record is kept of any third-party organisations who store, process or transmit Cardholder Data on behalf of the University, and/or who may otherwise affect the security of Cardholder Data;
- Ensure that appropriate due diligence has been carried out before entering into any agreement; this includes consulting with the Information Security team;
- Ensure Finance Division are aware of, and have formally approved, their use as a third-party service provider;
- Ensure that suitable clauses are included in the contract to ensure that PCI DSS responsibilities and requirements are clearly laid out; and
- Obtain proof of PCI compliance from any such third party on an annual basis and/or when requested to do so by the Finance Division for audit purposes.
3 CARDHOLDER DATA SECURITY PROCESSES

3.1 INTRODUCTION TO THE CARD HANDLING PROCESSES

Card fraud resulting from the compromise of data associated with a cardholder account is a significant criminal activity. As a result, when handling payments by card, the University is required to ensure ongoing compliance with the Payment Card Industry Data Standards (PCI DSS).

To ensure each unit that handles card payments meets our obligations under PCI DSS, the following guidance details how to implement the Payment Card Handling Rules. These rules and processes in relation to the obtaining, transmission and storage of customer card data, must be observed by all units who handle card payments.

Guidance from the Cashiers department (cashiers@admin.ox.ac.uk) must be sought in setting up any payment card handling process.

3.2 METHODS OF OBTAINING CARDHOLDER DATA

3.2.1 Customer Present Payments

This is a preferred method of obtaining Cardholder Data as the customer enters their card details directly into the device. This method is typically used in shops and other retail sites where the customer is present. The devices may be fixed to a location or mobile within the premises and they can be standalone or linked to an approved EPOS (electronic Point of Sale). Please contact the Cashiers office on how to obtain a Chip & PIN device.

- Only Card terminals obtained through the Cashier’s office may be used.
- When installing a Payment device you must consider how access is secured during short absences (putting it out of sight) and for longer absences, such as overnight when the device must be locked away.
- Card terminals must be protected from physical access by those not authorised to use the equipment.
- When not in use, card terminals must be physically locked away or locked down in till environments.
- As per Section 2.3.8, card terminals must be inspected at the beginning of each day for signs of tampering.

If you are running an event and want to be able to take card payments on site, the Cashiers Office have a fully portable terminal that can be used externally. Contact the Cashier’s office if you would like to use this facility at any time.

If you do not have a device for Face to Face payments, you should ask customers to use the relevant area of the University’s Online Store, which includes the facility to pay Invoices and make miscellaneous payments. Contact the Cashier’s office for details.

Please note that the Cashiers office will not take payments form customers phoning them directly.
3.2.2 Online Payments (Ecommerce)

The University’s Online Store is the preferred option for collecting online card payments securely. The Online Store can be used to sell goods and services, including courses and conferences. Please contact Cashiers to discuss alternative options available. Units wishing to set up a new ecommerce solution must obtain sanction from the Finance Division and Information Security beforehand, in order that due diligence can be carried out on the proposed supplier.

Details of approved suppliers can be found in Section 4.

University staff must not access out-sourced e-commerce solutions, such as WPM, on behalf of customers. If a customer payment cannot be taken by Chip & PIN, you cannot place the order on a University website on their behalf.

3.2.3 Mail Order Payments

When cardholder details are sent to the University by mail, the following processes must be observed:

- Appropriate arrangements must be in place for post opening, including the transfer of any details to the individual for processing without delay and suitable absence cover;
- The payment must be processed immediately via a Chip & PIN device, as a ‘cardholder not present’ transaction;
- The section of the document containing the card details must be cut off and destroyed using a cross cut shredder as per Section 2.3.18 – if necessary only the first 6 and last 4 digits of the card number may be retained in case of a query at a later date; and
- As detailed in Section 2.4.3, the 3 digit code (CVC/CVV2) must never be written down and must not be collected or requested on any forms.

3.2.4 Telephone Order Payments

When cardholder details are taken by telephone, the following processes must be observed:

- When setting up telephone order payment processing, the location of staff taking card information must be given careful consideration to ensure that it cannot be overheard by others not authorised to process payments.
- Ensure payment is taken in a secure manner:
  - If a Chip & PIN device (PED) is available, ask the cardholder to clearly state the 16 digit card number, the 3 digit authorisation code and the card expiry date, and enter this data on behalf of the customer using a ‘cardholder not present’ transaction;
  - If a Chip & PIN device (PED) is not available, transfer the call to a colleague with access to a working PED;
  - If no Chip & PIN devices (PEDs) are available, advise the customer to use the University Online Store whenever possible – there is a section of the Online Store enabling customers to pay an Invoice or make a miscellaneous payment; or
  - If none of the previous options are possible, request the customer call back later.
- Cardholder Data must never be written down.
3.2.5 Email

Cardholder Data must never be accepted by email. If unsolicited card data is sent in by email, then:

- Make a separate note of the sender’s email address.
- Delete the email from the recipient’s inbox.
- Delete the email from recipient’s deleted items.
- Reply in a new email stating that the University does not accept card details by email, and that the email has been deleted. Advise the customer of alternative ways of completing the transaction.

The details of University credit cards must never be sent via email.

3.3 Transferring Cardholder Data to Other Units or Teams

The transmission of Cardholder Data must be kept to an absolute minimum. Where necessary, observe the following:

- As per Section 2.4.3, the 3 digit code (CVC/CVV2) must never be written down and must not be collected or requested on any forms.
- As per Section 2.3.19, completed card authorisation forms must be delivered to the Cashiers Office by hand, by special delivery or by secure cash carrier – neither the internal University post nor scanned email copies may be used.
- Do not use a fax machine linked to the internal Chorus telephone system.
- A log must be kept of all items sent, and it is the responsibility of the originating unit to track the forms and ensure they have reached their destination and been processed.
- Original copies must be destroyed by cross-cut shredder as per Section 2.3.18.

This applies to any form containing Cardholder Data that may be transmitted and processed.

3.4 Storing Cardholder Data

As per Section 2.4.2, Cardholder Data must never be electronically stored on University systems. As such, this section refers to storage on paper forms and other media.

3.4.1 Receipt rolls from Chip & PIN devices

- Ensure that the transaction receipts produced by the card terminals do not include the 16 digit card number – full card data must not be stored.
- If the full card data is being printed, you must contact the Cashier’s office so the device can be re-configured.
- Receipts may only be retained for as long as there is a legitimate business requirement or up to a maximum of one year, whichever is shorter.

3.4.2 Cardholder Data forms

- As detailed in Section 2.4.3, the 3 digit code (CVC/CVV2) must never be written down and must not be collected or requested on any forms.
A maximum of the first 6 and last 4 digits of the 16 digit card number may be retained where there is a business need, and then only for as long as necessary.

Full card data must not be stored, including in transaction logs.

### 3.4.3 University Credit Cards

- University Credit Cards must be stored securely, with access restricted to the card holder or their authorised representative only.
- Never send card details via email.

For further information, please contact the Cashiers Office.

### 3.5 Controlling Access to Card Holder Data

No one may be given access to payment card information or processes without the documented approval of the process owner.

- Anyone involved in a payment card process or with access to a payment area must be vetted as they are handling confidential information:
  - Where appropriate, confirm references and perform identity checks:
    - This vetting applies for permanent, contract or volunteer workers who have access to payment processes.
    - Check whether the role already includes appropriate vetting such as DBS.
    - Contact HR for what checks are appropriate to the position.
  - A local log must be maintained of everyone in the unit who has been granted access to payment card data, including a record of when and who granted the access:
    - The log must record revocations of access, e.g. change of role or staff resignation.
    - This log must include a record of training in Payment Card handling and an acknowledgement by the person they have received training and acknowledge their accountability for compliance.
    - The log may be requested as evidence in an internal or external compliance audit.

### 3.6 Reporting Incidents Involving Cardholder Data

#### 3.6.1 Definition of an incident

An “incident” is defined as a suspected or confirmed “data compromise”. A “data compromise” is any situation where there has been unauthorised access to a system or network where Cardholder Data is collected, processed, or transmitted. For purposes of PCI DSS, a “data compromise” can also involve the suspected or confirmed loss or theft of any material or records that contain Cardholder Data.

Some examples of data compromise incidents that an employee might recognise in their day to day activities include, but are not limited to:

- Theft, damage or unauthorised access, such as papers missing from their desk, broken locks, missing log files, alert from a security guard, video evidence of a break-in or unscheduled/unauthorised physical entry;
- Fraud;
• Inaccurate information within databases, logs, files or paper records;
• Payment Card terminals (PEDs) that have been tampered with or substituted; or
• Computers that have a suspicious device inserted into a USB port.

3.6.2 Unit Incident Response

As per the requirements in Section 2.3:

• Any suspected incident involving PCI data must be reported to cashiers@admin.ox.ac.uk within 4 working hours of discovery and on the same working day wherever possible; and
• Any suspected incident which involves potential compromise of information systems, such as EPOS tills or e-commerce sites, must be reported to local IT support and to the Information Security team via oxcert@it.ox.ac.uk.

Units are additionally required to maintain local incident response procedures which include their requirements under PCI DSS. A template incident management policy and associated quick-reference chart are available from the Information Security Team website.

3.6.3 Cashiers Incident Response

As part of the response to any suspected incident involving PCI data, cashiers will:

• Confirm with the unit whether or not any information systems are involved, and if so verify that the Information Security Team has been notified;
• Work with involved staff, local IT support and the Information Security team as necessary to determine whether or not an incident has taken place;
• Where an incident involving PCI data is confirmed, work with units to implement any required incident response procedures mandated by the payment brand; and
• Where necessary, coordinate all communications with the payment brand.

3.6.4 Information Security Team Incident Response

As part of the response to any suspected incident involving the compromise of PCI data on Information Systems, the Information Security Team will:

• Confirm with the unit that the incident has been reported to the cashiers;
• Work with involved staff and local IT support to verify whether or not an incident has taken place; and
• Where an incident involving PCI data is confirmed, work with units to analyse and resolve the incident, and to determine corrective actions to avoid future re-occurrence.

3.7 Compliance with PCI & University Rules

An attestation of compliance must be carried out yearly by any unit handling payment cards, but the University Acquiring bank may carry out an audit at any time.

All units handling payment cards must be prepared to provide evidence of compliance for such an audit.

---

4 [https://www.infosec.ox.ac.uk/guidance-policy/incident-management](https://www.infosec.ox.ac.uk/guidance-policy/incident-management)
4 APPROVED SUPPLIERS AND SOLUTIONS

This list of approved suppliers and solutions is being reviewed during the PCI Compliance Project. This is the list as of the document date.

4.1 ECOMMERCE

<table>
<thead>
<tr>
<th>Process/ Transaction Type</th>
<th>Company</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Store</td>
<td>WPM</td>
<td>Contact Cashiers office for details.</td>
</tr>
<tr>
<td>Events / tickets</td>
<td>TBA</td>
<td></td>
</tr>
<tr>
<td>Room booking</td>
<td>TBA</td>
<td></td>
</tr>
<tr>
<td>Soliciting Donations</td>
<td>Development and Relationship System (DARS)</td>
<td>Contact UODO DARS team</td>
</tr>
<tr>
<td>Payment Processing</td>
<td>WorldPay</td>
<td>Contact Cashiers office for details.</td>
</tr>
</tbody>
</table>

4.2 FACE TO FACE

<table>
<thead>
<tr>
<th>Process/ Transaction Type</th>
<th>Company</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment Entry Device</td>
<td>Verifone</td>
<td>Contact Cashiers office for details.</td>
</tr>
</tbody>
</table>