PCI DSS Policy and Procedures

Policy Owner	Rachel Burgess, Head of Financial Control
Approving Body	Executive Board
Date of approval	6 October 2020
Deadline for review	6 October 2022

PCI DSS

Policy

1. Introduction

This policy and its associated procedures outline the College's management of payment card security as part of compliance with the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS is a set of standards to help protect people from cardholder data theft or fraud. They represent the minimum standards of security required to safeguard payment card transactions. PCI DSS applies to all organisations that store, process or transmit cardholder data.

Failure to comply with PCI DSS could result in financial penalties, costly investigations and damage to the College's reputation.

This policy should be read in conjunction with PCI DSS Procedures and the College's Cyber Security Policy and Data Management Policy.

2. Scope

PCI DSS applies to all types of card payments: online, post, over the phone, or face to face via card machines. For the purposes of this policy, cardholder data includes the following:

- the Primary Account Number (PAN)
- cardholder name
- expiry date
- security code
- chip or magnetic strip data
- three-digit code (e.g. CVC code)
- PIN

The policy applies all staff, including student workers, handling cardholder data, exposed to the handling of cardholder data, or who have a role in payment processing in any capacity.

There are detailed PCI DSS procedures associated with this policy that cover the following:

- Key elements of cardholder data security
- Key processes for 'face to face' transactions (e.g. paying by card at a College outlet)
- Key processes for 'cardholder not present' transactions (e.g. processing payments by phone, mail)
- Key processes for using terminals, including 'tamper checks'
- Incident response

This policy relates to Royal Holloway only, and scope does not extend to the Students' Union.

The scope for the Card Data Environment is expected to be that no data is stored by the College, as this is outsourced to third parties, such as WPM. Any changes to this must be notified to the PCI DSS team.

3. Policy statement

The College will comply with the PCI Security Standards (v3.2.1) covering the following 12 responsibilities:

Goals	
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for employees and contractors

4. Training

Training must be completed by all staff (including student workers) handling cardholder data, exposed to the handling of cardholder data, who work in the environment where these activities take place, or who have a role in payment processing in any capacity. Training can be accessed on Moodle and must be completed prior to starting work, and refreshed at least annually.

Line managers are responsible for ensuring their staff have read and understood the PCI DSS policy and procedures and have undertaken applicable training. Line managers are responsible for recording and reporting compliance with training.

Unsuccessful or incomplete training must be recorded and the staff member barred from accessing Card Holder Data (CHD) until it has been successfully completed.

Staff who do not comply with the requirements of the training and the College's PCI DSS policy and procedures may be subject to College disciplinary procedures.

5. Roles and responsibilities

Line managers and staff are responsible for managing PCI DSS "business as usual" activities daily (e.g. tamper checks on devices).

A PCI DSS team will be responsible for:

- overseeing PCI DSS compliance overall
- performing quarterly reviews of PCI DSS scope (identifying all in-scope and out-of-scope networks and system components, and all connected third parties
- performing quarterly scans of any cardholder data retention, wireless access points, adherence with procedure, and to ensure quarterly vulnerability scans have taken place in line with the PCI DSS standards
- reviewing training materials and completion rates at least annually
- reviewing controls and procedures in place at least annually
- preparing and testing the incident response plan at least annually
- confirming receipt of third party Attestation of Compliance documentation annually.

The team will comprise:

Core members:

- Finance SMT member, e.g. Head of Financial Control or other Finance SMT member
- Commercial Services Finance representative, e.g. Financial Performance Manager
- IT representative
- Internal Security Assessor, e.g. Head of Business Applications

By invitation:
Representatives from: Network team, Student Fees, Development, Cyber Security, Compliance and Data Protection, Security

There will be a central email for PCI DSS issues that will be monitored jointly by the core members of the team pcidss@rhul.ac.uk

6. Attestation of compliance

The College will evidence compliance annually by the completion of an Attestation of Compliance. This may be completed by an external Quality Security Assessor or an Internal Quality Assessor.

PCI DSS

Procedures

Contents

1. Introduction

These procedures should be read in conjunction with the PCI DSS Policy. They cover the PCI DSS standards relating to the protection of cardholder data and the restriction of access to cardholder data, including the following:

- Key elements of cardholder data security
- Key processes for 'face to face' transactions (e.g. paying by card at a College outlet)
- Key processes for 'cardholder not present' transactions (e.g. processing payments by phone, mail)
- Key processes for using terminals, including 'tamper checks'.
- Incident response

The following elements of PCI DSS standards are covered by IT-related policies such as the Cyber Security Policy:

- Build and maintain a secure network
- Maintain a vulnerability management programme
- Regularly Monitor and Test Networks

2. Training

Training must be carried out by all those handling cardholder data, exposed to the handling of cardholder data, who work in the environment where these activities take place, or who have a role in payment processing in any capacity. Training can be accessed on Moodle and must be completed prior to starting work, and refreshed at least annually.

Line managers are responsible for ensuring their staff have read and understood the PCI DSS policy and procedures and have undertaken applicable training.

Staff who do not comply with the requirements of the training and the College's PCI DSS policy and procedures may be subject to College disciplinary procedures.

3. Card payments received by the College

Card payments are received by the College either online, through a College-approved compliant e-payment system (e.g. WPM payment system, Blackbaud or the online store), or by using card payment devices.

When payments are received through the online payment system and online store, no card details are to be retained by the College and there must be no access to full card details by any member of staff.

Any third party that stores, transfers or process cardholder data on behalf of the College must be PCI DSS compliant as evidenced by an Attestation of Compliance supplied to the College. This includes any websites involved in payment

acceptance, any tablet or mobile phone apps, any software or online booking service providers.

For card payments received through payment devices, there are strict processes that must be adhered to in order to achieve PCI DSS compliance. These are set out below.

4. Key elements of cardholder data security

The key overarching elements of maintaining cardholder data security are as follows. These are described in further detail in the sections below.

- No staff member should handle cardholder data unless there is a business need, they have authorisation to do so and they are appropriately trained.
- Where call campaigns are carried out all staff must be trained beforehand, and systems set up to ensure the PCI DSS policy and procedures can be followed.
- Cardholder data should never be stored electronically unless in accordance with this policy.
- Paper records should be avoided. Any paper records held should be destroyed securely (i.e. shredded) as soon as a transaction is processed.
- Payment details should never be sent by electronic messaging such as emails, texts or other electronic services.
- Card details should never be sent to another department by internal mail.
- Cards should never be copied by scanning or similar.
- Payment terminals should be checked at least daily (tamper checks).
- **Only authorised people who have received training can process payments.**
- **Any concerns are always reported immediately to a line manager or directly to the PCI DSS team.**

5. Types of card transactions

There are two types of payment processing at the College: 'Face to Face' and 'Card Not Present'.

A **'Face to Face'** transaction is where the customer presents their card to make a payment, which is processed by a member of College staff. Face to face payments will only be taken via a payment device (sometimes known as a PDQ), or an integrated till (EPOS system).

A 'Card Not Present' transaction is where the customer and their payment card are not present at the point of sale. This will occur where details are provided over the phone, or via post. The payment is then processed via a payment device, or on an online payment system such as Blackbaud.

6. Key processes for Face to Face transactions

The following processes must be followed by any staff handling face to face transactions:

- Do not touch the card unless the customer is having difficulties and offers it to you.
- Keep the card in the customer's sight at all times.
- Be aware of other customers 'shoulder surfing' or using phone cameras to steal customer card data.
- Be aware of any security cameras that could view customer card data – report to your line manager you are concerned that this is an issue.
- If you cannot process the transaction immediately, the customer must return later – do not write down the card details.
- When a payment is processed the paper 'merchant copy' receipt generated by the machine should be stored securely and the 'customer copy' handed to the customer. If receipts need to be retained for business reasons, they must be stored securely. All receipts must only be printed with truncated card details.
- If a lost payment card is found it must be immediately stored in a sealed envelope and placed in a secure till, locked drawer or locked cash box. If a secure location is not available the card must be destroyed immediately. Should the card be claimed, photo ID must be seen (e.g. driver's license, passport) and details should be documented:
    - Who found the card
    - Where it was found
    - Who it was reported to
    - Who claimed the card
    - What ID was checked

7. Key processes for Card Not Present transactions

Card not present transactions may be processed by telephone or by mail.

Should card details be received by email or other electronic messaging, the incident should be logged, and then the email should be immediately deleted (from inbox and trash/recycle bin) and payment should *not* be taken using the emailed details. The cardholder details must not be written down. The customer must then be informed (in a new email) that their card details cannot be accepted this way.

NB Do not use 'reply' as you may inappropriately transmit cardholder data.

7.1 Card Not Present - telephone

The following processes must be followed by any staff handling Card Not Present transactions via telephone:

- Wherever possible cardholder details are entered directly into the payment terminal or online system (e.g. Blackbaud) with no need to write down the details.
- Be aware of people who can overhear you.
- Never read back the card number. Ask the customer to repeat their number if necessary.
- Never ask for 3D Secure or Verified by Visa codes, when processing through an online interface.
- Calls must only be made on an approved secure telephone – mobile phones should not be used for outbound calls.
- Do not use wireless headsets when taking telephone payments as Bluetooth is not considered secure – wired headsets must be used.
- No voice recordings of cardholder data shall be made. Ensure phone calls involving card data are not recorded.
- Avoid taking notes of cardholder data during calls. If notes of cardholder data are made, make sure they have been destroyed securely in a crosscut shredder as soon as the transaction is complete. Placing in the confidential waste bin is not appropriate, a shredder must be used.
- In exceptional circumstances, if it is not possible to process the payment immediately, the card details may be written down (but not the 3-4 digit security code) and processed later. These notes must be immediately locked away (e.g. in a locked cabinet, in a room which must be locked when unoccupied). Once processed they must be securely destroyed using a crosscut shredder. Placing in the confidential waste bin is not appropriate, a shredder must be used.
- Where call campaigns are carried out all staff must be trained beforehand, and systems set up to ensure the PCI DSS policy and procedures can be followed.

7.2 Card not present – mail

Normally cardholder details should only be accepted on paper where there is no other viable method of payment. Where payments can be made online or face to face, this should be encouraged. Where cardholder data is received through the mail:

- The payment details must be delivered to a secure mail location, such as a locked post box.
- The mail must be picked up daily, by authorised staff members only.
- Such mail should not be transferred via internal post but should be delivered in person by someone authorised to do so.
- Paper forms must not collect the CVC number.
- Staff must be aware of signs of the mail having been tampered with, e.g. being resealed.
- Payment should be processed immediately.

- The payment details should be entered into an online system or input into a Process Data Quickly (PDQ) terminal.
- Payment instructions received on paper are then destroyed securely using a crosscut shredder. Placing in the confidential waste bin is not appropriate, a shredder must be used.
- If payment cannot be processed immediately, the details may be securely locked away (e.g. in a locked cabinet or safe, in a room which must be locked when unoccupied).
- Sensitive authentication data must never be stored on paper (full magnetic stripe data or equivalent on a chip, CAV2/CVC2/CVV2/CID or PINs).
- Once processed, payment details must be securely destroyed using a crosscut shredder. Placing in the confidential waste bin is not appropriate, a shredder must be used.
- Normally cardholder details would *not* be collected on paper at events.

8. Payment devices

8.1 What are payment devices?

Payment devices may be known by different names, such as:

- PED (PIN/Payment Entry Device)
- Chip n PIN
- PDQ (Process Data Quickly)

There are different types of payment devices:

- Connected by GPRS (General Packet Radio Services) – these are not connected to the College network.
- P2PE devices (point-to-point encryption) – these are connected to the College network but are encrypted to ensure the network is out of scope for PCI DSS.
- Some devices are connected to a till (sometimes known as EPOS (Electronic Point of Sale) – this avoids manual entry of the sale amount for each transaction.

The details (make, model, serial number, description, security features, location, and device supervisor) of all payment devices in use must be recorded.

8.2 Key processes for using payment devices

- No payment devices will be connected to the College's network unless they are properly end-to-end encrypted (e.g. P2PE devices).
- Payment devices should only be used by authorised and trained staff.
- Payment devices should be checked daily for evidence of tampering (see below).
- The payment device should be visible to staff at all times and therefore difficult for others to access unobserved. The device should be in a position

where it is easy for staff to observe – but difficult for others to touch unnoticed.

- Payment devices should be secured/locked down when unattended.
- The device must only print the last four digits of the payment card Primary Account Number (PAN) on receipts.
- Ensure visitors to areas where devices are used are expected and have the right credentials.
- Ensure the identity (vendor issued photo ID and Government issued ID such as a driving license) is checked for anyone who asks to check the terminal (for example, this could be a criminal posing as an engineer).
- Watch out for anyone hanging around the device in a suspicious manner.
- Be aware of other customers 'shoulder surfing' or using phone cameras to steal customer data.
- Be aware of any security cameras that could view customer card data – report to your line manager you are concerned that this is an issue.
- Keep the card in the customer's sight at all times.
- Do not touch the card unless the customer is having difficulties and offers it to you.

8.3 Tamper checks

The payment device is a target for criminals trying to steal cardholder data. They may attempt to modify the device or add something to it to enable them to record card data as it is processed. Devices can effectively be replaced by criminals and then cardholder data can be siphoned off for months afterwards.

As well as the physical security measures outlined above, payment devices should be checked daily for evidence of tampering or anything suspicious. The following should be checked daily:

- Has the serial number or other ID labels changed?
- Have the labels been moved or possibly peeled off?
- Do the screws or the device case show signs of damage or being forced?
- Have cables changed?
- Are there any attachments to the device?
- Is the display different?
- Has the format of receipts changed?
- Is the card slot different or does the card not fit as is used to?

If there is a fault with the device report this to the supplier by calling the phone number listed on the underside of the device.

However if you are at all *suspicious* you must report this. Stop using the device and let other people know not to use it. Contact your line manager who will report to the PCI DSS Team.

9. Incident response

An "incident" is defined as a suspected or actual situation where there has been unauthorised access to a system where cardholder data is collected, processed, stored, or transmitted. This can involve suspected or actual theft or loss of any records that contain cardholder data. Examples may be, inter alia, evidence or suspicion of device tampering, a report of an incident from a third party or cardholder, theft of a device, etc.

Employees are responsible for reporting incidents to their Line Manager.

The Line Manager will then inform the Incident Response Team (PCI DSS team) who will initiate the incident response process

If you become aware of a suspected or real security incident relating to cardholder data, or a failure in procedure, then you must act immediately.

The Incident Response Team will comprise the main PCI DSS team with others by invitation as necessary depending on the incident. The team will meet annually to review and test incident response procedures.

9.1 Incident response process

When an incident is reported the Incident Response Team will:

- Ensure where possible that no further payment can be made through the affected channel.
- If relating to a device, ensure it is not shut down or unplugged but ensure no-one uses the device.
- Conduct an initial investigation of the suspected incident, utilising as necessary CCTV, IT system logs and alerts, access control logs and interviews with staff.

If the incident involves the compromise of card account numbers, the Incident Response team will:

- Contact Network Services and Information Security to contain and limit the exposure by shutting down any processes or systems affected by the compromise.
- Alert necessary third parties (e.g. acquirer, bank, credit card issuer, the Police, reporting bodies such as Information Controller or OfS).
- Provide compromised or potentially compromised card numbers/details to the relevant parties as soon as possible.
- Ensure there is an internal communications plan.
- Document every decision and action taken.

After the incident the College's response will be reviewed and procedures updated as appropriate.

Appendix A: Glossary of terms

Cardholder Data – Payment card data including Primary Account Number (PAN), name of cardholder, expiration date and service code.

CAV2/CVC2/CVV2/CID – 3-digit security code displayed on payment cards.

EPOS – Electronic Point of Sale

PAN - A "Primary Account Number" is a 14 or 16 digit number embossed on a debit or credit card and encoded in the card's magnetic strip which identifies the issuer of the card and the account.

Payment card - A card backed by an account holding funds belonging to the cardholder, or offering credit to the cardholder such as a debit or credit card.

PCI DSS - The Payment Card Industry Data Security Standard

PDQ Machine – A credit card swipe machine (Process Data Quickly)

PED – PIN Entry Device.

PIN - A "Personal Identification Number" is a secret numeric password used to authenticate payment cards.

SAQ – Self Assessment Questionnaire to evidence compliance.

Sensitive Authentication Data - Full magnetic stripe data or equivalent on a chip, CAV2/CVC2/CVV2/CID or PINs/PIN blocks.

Stripe / track data - Information stored in the magnetic strip or chip on a payment card.