Goldsmiths
UNIVERSITY OF LONDON

PCI-DSS Compliance Policy

Contents

Ownership	Chief Financial Officer
Policy contact	Jamie Warner
Approval	Audit and Risk Committee
Protective Marking	Public
Last review date	February 2025
Next review date	February 2028

1 PCI-DSS Compliance Policy

1.1 Introduction

PCI DSS stands for Payment Card Industry Data Security Standard. It is a set of security standards and guidelines designed to ensure the secure handling of credit and debit card information. PCI DSS was developed to help organizations that process card payments prevent data breaches and protect cardholder information from theft and fraud.

1.2 Founding Members

PCI DSS is a worldwide security standard assembled by the Payment Card Industry Council with the council's five founding members being:

- Visa Inc.
- American Express
- Discover Financial Services
- JCB International
- MasterCard Worldwide

It aims to assist Goldsmiths in reducing debit and credit card fraud by implementing enhanced controls around payment transactions. This standard applies to all organisations that handle, process, store, or exchange cardholder information, regardless of whether it is done digitally or manually. Non-compliance with PCI DSS can result in the loss of the ability to process card payments, fines, and reputational damage.

1.3 Scope

This policy covers the requirements for all payment card processing activities across Goldsmiths, both manual and IT-based, and applies to all staff involved in card payment processing.

Whenever possible, payment card data processing is delegated to third-party service providers accredited to handle such data in line with the PCI DSS standard. Goldsmiths aims to minimize its adherence to the PCI DSS standard by either transferring processing responsibilities to approved third-party service providers or eliminating business processes that necessitate card data processing by Goldsmiths.

PCI DSS standards are designed to protect the cardholder information of students, parents, donors, alumni, customers and any other individual or entity that utilizes a credit or debit card to transact business with Goldsmiths. This policy is intended to be used in conjunction with the complete PCI DSS requirements as established and revised by the PCI Security Standards Council.

PCI DSS comprises a minimum set of requirements for protecting cardholder data and may be enhanced by additional controls and practices to further mitigate risks. Below is an overview of the PCI DSS v4.0 requirements.

Build and Maintain a Secure Network	1. Install and maintain network security controls 2. Apply secure configurations to all systems components
Protect Account Data	3. Protect stored account data. 4. Protect cardholder data with strong cryptography during transmission over open, public networks.
Maintain a Vulnerability Management Programme	5. Protect all systems and networks from malicious software 6. Develop and maintain secure systems and software.
Implement Strong Access Control Measures	7. Restrict access to system components and cardholder data by business need to know 8. Identify users and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Log and monitor all access to system components and cardholder data 11. Test security of systems and networks regularly
Maintain an Information Security Policy	12. Support information security with organizational policies and programs.

2 Authorisation and Responsibilities

2.1 Training and Authorisation

This policy is mandatory for all College staff, and failure to comply may result in disciplinary action. Heads of Departments are responsible for ensuring that their staff members are aware of and adhere to this policy. Staff must consult with Finance before ordering Process Data Quickly (PDQ) machines or requesting logins to online card systems. Departments must not implement business processes involving card payments without prior consultation with IT & Digital Services (IT&DS), facilitated through Hornbill, for guidance. Estates must also be involved to certify the security of the site.

2.2 Training and Authorisation

Heads of Department are responsible for ensuring that all new and existing staff receive copies of relevant policies and training in PCI DSS requirements. A list of authorized staff members who routinely use devices to process payment cards, such as tills, Pin Entry Devices (PEDs), Process Data Quickly (PDQ) machines, etc., must be maintained by the department responsible for providing these services.

Compliance Oversight

The Finance department is responsible for ensuring that Goldsmiths is PCI DSS compliant, and it has the authority to remove any payment card processing activity. We have worked to reduce the risk of data theft and provide a secure payment environment for our customers. The consequences of a security breach resulting in customer card data being accessed by an unauthorised party can be wide-ranging:

- Inconvenience and distress to our customers – card data theft and fraud can be very distressing and take time to resolve.
- Financial: lost income – the College may lose money due to fraudulent transactions.
- Financial: sanctions – Goldsmiths could be fined if card data is lost.
- We could be assessed as a high risk, level 1 merchant. We would need to have external verification of our security, which would be expensive and time consuming for the College.
- The College could have its ability to take card payments removed. This would cause increased workload and could lead to loss of business.
- Reputational damage – this could be the most damaging consequence of all, as data security breaches tend to get a lot of publicity.

Complying with PCI DSS requirements does not guarantee that a security breach will not occur, but it reduces the risk, and our liability.

This policy is mandatory to all staff. Further information on PCI DSS can be obtained from the Security Standard Council webpages.

2.3 Network Security

IT&DS is responsible for conducting and assessing the results of external and internal network security scans required for PCI DSS compliance. These scans must be performed at least quarterly to evaluate security against external access to any networked devices processing payment card data and after any major system changes. Finance is responsible for maintaining an inventory of all devices used for payment card processing, including tills, PEDs, PDQ machines, etc.

2.4 Incident Response

In the event of a data breach, staff must follow the Data Breach Reporting Procedure.

3 Payment Card Processing

3.1 Online Payment Processing

Online payment processing is the preferred method for credit or debit card payments, as approved payment service providers handle cardholder data. Goldsmiths does not retain any card details processed through its approved online system, Global Pay. Whenever possible, students, staff, and customers should be directed to Goldsmiths' online payment services and online payment pathway facilities.

As per the financial regulations, where departments require the facility to take credit/debit card payments other than for the collection of student fees e.g. for transcript or conference payments, they should contact Goldsmith's Finance department initially to make the necessary arrangements. Departments must not make their own arrangements with Merchant Services Providers.

3.2 Protecting Online Payments - SSL Certificate / HTTPS

To protect our customers, where personal and payment details are to be entered for online payments, Goldsmiths' online payment pathway must have a valid Secure Sockets Layer (SSL) Certificate.

Having a valid SSL Certificate in place ensures that the required information should only ever be obtained via secure webpages beginning with the prefix **https://** and which allows for secure ecommerce transactions encrypting the data being entered.

3.3 In-person Card Transactions

Approved card processing terminals may be used when online payment processing is not feasible. The Finance team maintains an inventory of authorized tills and PDQ machines for card transactions. These devices must be reviewed and reviewed regularly by the Treasury Accountant. Card payments can only be processed using authorised devices. Line Managers must ensure that machines are not replaced, tampered with, or adjusted without prior approval.

Customer present card payments can be processed in two ways:

- Using Electronic Point of Sale (EPOS) systems with Point-To-Point-Encryption (P2PE) compliant terminals on separate VLANs.
- Using standalone PDQ terminals connected via analogue lines that do not use the network.

Card details must never be written down by staff for future payment attempts.

The College may screen users of PDQ machines, or anyone expected to understand the rules of PCI-DSS compliance, by performing spot checks on card machines, and checking staff members' e-learning records for evidence the online course has been completed.

Goldsmiths will contractually require all third parties with access to cardholder data to adhere to PCI DSS and Data Protection requirements. These contracts will clearly define information security responsibilities for contractors. Third parties will be required to prove their own compliance with PCI DSS and must continue to do so upon request – this includes proving compliance for any kiosks or devices supplied.

Third parties include:

- Resellers
- Till vendors
- EPOS vendors
- Software application providers
- Payment services providers
- Payment processing bureaux
- Data storage providers
- Web hosting providers
- Shopping cart providers
- Software vendors

Third party PCI Service Providers should also be able to be found via the following Visa website: https://www.visa.com/splisting/searchGrsp.do

Goldsmiths also has catering and conference outlets – in these cases, an outside contractor maintains all card payment processing responsibilities.

3.4 Other Card Transactions

3.4.1 Request by Telephone

In no circumstances should Goldsmiths' staff ask for card details received over the telephone. Instead, students should pay using the variety of payment options available on Goldsmiths' How To Pay section of our website.

3.4.2 Card Details Received In Writing

Goldsmiths' staff should immediately shred any card details received in writing or via email.

Cardholder data (CHD) includes the full card number (PAN), cardholder name, expiration date, and service code. CHD may be stored for regulatory and legal requirements and business use but must be rendered unreadable using methods like hashing, truncation, and encryption. The full PAN must not be retained.

Sensitive authentication data (SAD) includes full track data, CAV2/CVC2/CVV2/CID numbers, and the personal identification number (PIN). SAD should never be stored after payment authorization.

Receipt of CHD by email is a violation of PCI DSS, as it is an unsecured channel that can be intercepted. Any card holder data received in this format must not be forwarded and must be deleted immediately.

Storage of cardholder data on PCs in any format (email, databases, spreadsheets, pen drives, etc.) is prohibited as it breaches security regulations and makes Goldsmiths non-compliant, potentially leading to fines from card brands. Routine audits will ensure compliance with this condition.

3.5 Refunds

3.5.1 Online refunds

Refunds must be approved by the appropriate authorised signatory in accordance with the refund procedures for Goldsmiths online system being used. The appropriate system is then accessed by the nominated College person(s) and the refund is processed back to the source card from which the original transaction was authorised.

For Goldsmiths online sites using Flywire or Convera, refunds can be processed back onto the original source card within 365 days of the transaction being taken as recommended by Worldpay.

If in any doubt about your online system uses, please refer to the PCI DSS Compliance Officer (currently the Head of Financial Operations).

After the above refund timescales, the customer should be contacted for alternative details for the refund to be processed either by BACS or bank transfer payment via our Accounts Payable department.

3.5.2 PDQ Terminal Refunds

PDQ refunds are required to be authorised on the PDQ terminal using a “Supervisor PIN or Password”. This PIN / Password must be kept securely by the nominated terminal users. If presently you do not use a “Supervisor PIN nor Password” you should contact cashoffice@gold.ac.uk to arrange to setup a PIN number or password for your terminal and to restrict its use where refunds are concerned only to the appropriate and necessary users.

Refunds should only be processed through the PDQ terminal back onto the source card from which the original transaction was authorised.

Refunds should under no circumstances be processed onto a card if the original payment was not processed through your terminal. Card scheme rules state that refunds should only be processed on a credit or debit card where there is a corresponding sale. If the source card is unavailable for the refund to be processed, then the customer should be contacted for alternative details for the refund to be processed by BACS or bank transfer via Accounts Payable.

The merchant banks we use to accept card payments also monitor refund transactions and may flag up any refund transaction that contravenes the card scheme rules, i.e. where a refund has been paid to a card without an original corresponding sale. In certain circumstances our merchant banks may choose to destroy a batch containing such an erroneous transaction which could impact on other sales made within the same batch.

A refund must never be processed onto a card that is not the source transaction card.

4 Terminal Security

4.1 Allowed Devices

Only approved devices and components are purchased by Goldsmiths to ensure compliance with PCI DSS security requirements for point-of-sale devices. Any requests for new or replacement devices must be made through the relevant PCI DSS Contact Officer (refer to Appendix 1).

All terminals owned by Goldsmiths are logged in Goldsmiths' PCI Devices Inventory. The inventory should be updated for any known changes, and the relevant PCI DSS Officer, by default the Head of Financial Operations, is responsible for maintaining the Inventory biannually.

Devices used to process payment cards, such as tills, PEDs, and PDQ machines, must:

- Only be used by staff who are trained and authorized for such duties.
- Be protected from physical access by unauthorized users outside of working hours. Small devices like PDQs should be securely locked away, while larger devices like tills should be kept in restricted access areas when not in use.
- Undergo routine visual inspections each day before use, with equipment, cabling, and connections checked for signs of tampering. The line managers of those staff members involved in using or maintaining payment equipment are responsible for maintaining a log of visual inspections.
- Not be taken off-site for testing, repair, or use without explicit approval from the relevant PCI DSS Contact Officer (Appendix 1).

Visitors to areas with access to payment equipment outside of working hours must be supervised, and details of such visits must be logged.

The installation of new or replacement equipment must be validated and approved by the Head of Financial Operations in coordination with IT&DS to ensure the security of payment equipment.

Payment devices must not be positioned where College CCTV cameras can record card numbers, PINs, or secure card data.

Finance will provide training for operators to ensure awareness of terminal security, and line managers are responsible for ensuring that all authorized operators complete the online e-learning.

4.2 Terminal Responsibility

Once a department has been provided with a PDQ terminal it is that department's responsibility to always ensure its safekeeping until such time as the terminal is either returned to Finance or the terminal provider. These PDQ terminals should be kept in a locked, secure location to restrict unauthorised access.

If there are changes occurring within the department the PDQ terminal must be always kept track of and should not be left in a situation whereby there is a lack of terminal ownership which could leave it vulnerable to abuse. If no longer required, the terminal should be returned to Finance immediately.

Alternatively, if there has been a change of terminal ownership within a department the appropriate Finance person in Point 6 must be informed.

4.3 Destruction of Cardholder Data (CHD)

CHD must be securely deleted or destroyed when no longer needed for legal, regulatory, or business purposes, with the goal of minimizing unnecessary data storage. When data is stored before destruction, it must be locked in a secure area with restricted access. Team members requiring access should be documented, and a process for maintaining this information securely should be established.

Audits conducted by the Finance team will ensure that CHD is not retained without an approved and documented secure storage process, and that data retention does not exceed legal requirements.

Hardcopy materials must be shredded using a cross-cut shredder and then disposed of through confidential waste disposal, incineration, or pulping to prevent the reconstruction of CHD.

All individuals handling CHD must receive training on the safe storage, retention, and destruction of CHD as part of their induction and PCI DSS awareness training.

5 Compliance and Monitoring

5.1 Compliance

All payment card processing activities within the College must comply with PCI DSS. All departments must adhere to the policy set out by the PCI Council to minimize risks to customers and to Goldsmiths. PCI-DSS stands for Payment Card Industry – Data Security Standards and is a set of rules we must obey when processing credit/debit card payments.

If you have difficulties implementing or complying with any aspect of this policy you should contact the PCI-DSS Compliance Officer, by default, the Head of Financial Operations.

Any staff or students including all permanent (direct hire), temporary and contract staff are responsible for ensuring our adherence with this policy. IT&DS (the Information Security Manager) and the Head of Financial Operations shall ensure it is available and promoted to those that need to see it.

It is the responsibility of the PCI-DSS Compliance Officer within Finance to maintain this policy and ensure it is reviewed regularly, or if the environment changes. An assessment of the risks relating to the processing of cardholder data will be conducted regularly by Finance with the support of IT&DS and Financial Operations. This assessment includes a stock check of devices, an PCI-DSS e-learning completion audit for all card reader users, and an assessment of device storage and card reader practice.

The PCI DSS Internal Security Assessor, Information Security Manager, Head of Finance Operations, or any of their representatives, are authorised to inspect any systems, databases, or physical areas of the College where cardholder data might be processed or stored.

Many areas of the College process credit/debit cards as payment for the services they provide. Separate Merchant IDs (MIDs), set up by our acquiring bank have been authorised for use by a number of Departments. All relevant Heads of Department are responsible for ensuring that this policy is adhered to, that only College-approved devices and suppliers are used to receive payments, and that each MID has an identified and responsible manager.

The PCI-DSS Compliance Officer is responsible for maintaining a full register of all MIDs, the manager responsible, and all assets in use relating to each MID (e.g. point-of-sale / PDQ terminals).

Non-compliance may lead to fines and restrictions on transactions by Visa, MasterCard or China Union Pay.

The Finance team will initiate the requirement for an annual assessment to ensure ongoing compliance and perform checks and audits of the College's systems and processes to identify non-compliance, threats, and vulnerabilities. For inquiries or compliance issues related to this policy, please contact a member of Finance via cash-office@gold.ac.uk.

5.2 Monitoring and Training

All individuals handling CHD must receive training on the safe storage, retention, and destruction of CHD as part of their induction and PCI DSS awareness training. This training will be delivered via e-learning.

All staff members that take credit/debit card payments for the College are responsible for ensuring that they have completed the necessary online training before they can take payment.

6 Contacts

6.1 Contacts

The departmental contacts are as follows:

IT: infosec@gold.ac.uk
Finance:
Head of Financial Operations, j.warner@gold.ac.uk
Treasury Accountant, m.garba@gold.ac.uk
.

Document history

Version	Date	Details	Author	Approved
1.0	26/02/2025	Reviewed by Audit and Risk Committee	Jamie Warner	26/02/2025