QUEEN'S UNIVERSITY BELFAST

Payment Security Policy

Version	Reviewer	Approval / Changes	Date
1.0	PCI DSS Compliance Group	University Operating Board	October 2015
2.0	PCI DSS Compliance Group	Minor amendments to reflect UOB comments and addition of User Group Terms of Reference	May 2016
3.0	PCI DSS Compliance Group	Minor amendments	May 2017
4.0	PCI DSS Compliance Group	Minor amendments	May 2018
5.0	PCI DSS Compliance Group	Minor amendments	May 2019
6.0	PCI DSS Compliance Group	Minor amendments	May 2020
7.0	PCI DSS Compliance Group	Section 4.3 updated and other minor amendments	May 2021
8.0	PCI DSS Compliance Group	Section 4.1.4 updated and other minor amendments	May 2022
9.0	PCI DSS Compliance Group	Section 5.3 added and other minor amendments	March 2024
10.0	PCI DSS Compliance Group	Policy renamed, Section 4 updated and other minor amendments	March 2025

Index

1. Introduction and Policy Statement

1.1 Content and Scope

The Payment Card Industry Data Security Standard (PCI DSS) is a worldwide information security standard created to help organisations which process card payments to prevent credit and debit card fraud. This is achieved through tight controls surrounding the storage, transmission and processing of cardholder data. The PCI DSS applies to all organisations which receive, process, store and transmit cardholder information.

The purpose of the payment security policy is to ensure that the University is compliant with PCI DSS. The processing of credit and debit card data, within the University, must comply with the conditions set out within this document. It is also University policy that wherever possible, the processing of credit and debit card data should be sub-contracted to third-parties who are licensed or accredited to process such data in line with the PCI DSS, e.g. Payment Service Providers (PSP).

The University seeks to eliminate processing of credit and debit card data through its infrastructure – transferring that responsibility, and the requirement to be PCI DSS compliant, to the relevant PSP. In this regard, the University will take steps to ensure that it minimises the scope of the PCI DSS to which it must adhere, either by transferring that processing to a licensed PSP, or by eliminating business processes which require the processing of card data by the University.

The University is liable to fines from its merchant bank should it fail to comply with PCI DSS. Failure to comply may also result in Visa and/or Mastercard preventing transactions from being processed by the University.

1.2 Where the policy applies

The policy applies to all locations and areas, within the University, which use processes involving card data.

1.3 Intended Audience

Compliance with the policy is mandatory for all staff. Failure to comply may result in disciplinary action. Faculty Pro-Vice Chancellors/Directors are responsible for ensuring that their staff are aware of the policy and that it is adhered to. Faculties/Directorates must not implement business processes which involve the processing of card data, without first consulting with the PCI DSS Compliance Group who will advise on how such data should be processed.

1.4 Other Relevant Policies

This policy should be read in conjunction with the following University policies, guidance and procedures:

- Information Security Policy
- Information Handling
- Mobile Computing Policy
- Data Security Guidance
- Password Policy
- Guide to Encrypting Data
- Data Protection
- Fraud
- PCI DSS Incident Response Plan

Note that the University does not store, process or transmit cardholder data so a separate policy for cardholder data is not required.

Further external guidance can be found at www.pcisecuritystandards.org.

1.5 PCI DSS Compliance Group

A PCI DSS Compliance Group, comprising members of the Finance, Student & Campus Life, Digital & Information Services and the University Secretary's Office, is responsible for ensuring compliance with the PCI DSS and ongoing adherence to the Policy. The group can be contacted on their Microsoft Teams site at PCI DSS Compliance Group.

2. Security Breach of Credit and Debit Card Data

2.1 A security breach of credit and debit card data arises when card data is lost. Data breaches do occur regularly and e-commerce sites are a frequent target from hackers who often successfully compromise e-commerce sites. It is therefore imperative that all the relevant controls are implemented and adhered to in full.

2.2 In the event of there being a security breach of credit and debit card data, staff must follow the procedures outlined in the PCI DSS Incident Response Plan.

The PCI DSS Group may then advise if card data processing should:

- continue without change;
- continue, subject to the implementation of agreed actions; or
- be suspended, with immediate effect.

Credit and debit card data is personal data as defined by the UK General Data Protection Regulation and Data Protection Act 2018. The PCI DSS Incident Controller will also contact the Data Protection Officer c/o the Information Compliance Unit on info.compliance@qub.ac.uk as soon as possible if a breach arises, as the University would also have to make a decision as to whether the UK Information Commissioner should be advised.

3. Online Payments

3.1 It is University policy that online payments using credit and debit cards must be sub-contracted to third-parties who are licensed or accredited to process such data in line with the PCI DSS such as licenced Payment Service Providers (PSP).

3.2 The University will secure independent verification of the credentials/certification of a third-party provider, to ensure they have the necessary qualification to provide PCI DSS processing services. A record of the independent verification will be maintained.

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

3.4 For all card details which are processed through an online system, no card details will be retained by the University. There is no University access to full card details, as this information is stored on an external encrypted PSP server.

3.5 Schools or Directorates must not implement business processes or systems which involve the taking of payments and processing of card data, without first consulting with the PCI DSS Compliance Group, who will advise on how data should be processed and requirements that should be included in a tender exercise. It is recommended that payment applications have been validated as compliant with the PCI DSS Software Security Framework which replaced PA-DSS in October 2022.

3.6 Students must not be specifically directed to University IT equipment to use University provided online payment solutions. If a student wishes to use University IT infrastructure to make an online payment, then it is their choice (and at their own risk) and should not be mandated by the University.

3.7 Computers must not be used by University staff to access outsourced e-commerce solutions, such as WorldPay, Blackbaud or Shopify on behalf of customers.

3.8 University staff may only use PED (chip and PIN) machines to make payments on behalf of customers.

4. Card Payment Terminals – Chip and PIN Machines

4.1 Chip and PIN Machines

4.1.1 The use of Chip and PIN machines must be authorised by the PCI DSS Compliance Group and should be P2PE devices where possible. Standalone P2PE devices will be ordered from Worldpay while P2PE devices integrated with an e-POS solution will be ordered through the e-POS provider.

4.1.2 Chip and PIN machines must be set up following the instructions on the P2PE Implementation Manual (PIM) that should be provided in advance of the machines being used for the first time. The devices should not be purchased without contacting a member of the Payment Security team in Student Finance.

4.1.3 The merchant copy receipt should be held in a secure location.

4.1.4 The Permanent Account Number (PAN) (16 digits) must be redacted from the merchant copy receipt. This can be done by contacting Worldpay or Windcave support helpdesks. It is particularly important that this step is done when new terminals are delivered or when faulty terminals are replaced.

4.1.5 Copies of the merchant copy receipt should only be retained for necessary business purposes such as income reconciliation and must be securely disposed of as soon as such reconciliations are complete. It is recommended that receipts are not held any longer than quarterly.

4.1.6 Hard-copy materials must be shredded, incinerated, or pulped so that cardholder data cannot be reconstructed by staff who are responsible for card transactions.

4.2 Other methods of processing card details

4.2.1 Card details must never be received or transmitted by post or messaging technologies (for example, e- mail, instant messaging, SMS, chat, VoIP, etc.).

4.2.2 Any card details received by messaging technologies should be hard deleted immediately and the customer advised to use another channel – online, phone or on site. Do not reply to the customer using the inbound email which included the card details; use a fresh email to inform the customer it is against University policy to accept cardholder information in an email and we cannot process the transaction using details received in this manner.

4.3 Telephone payments

4.3.1 Telephone payments should only be taken on the dedicated secure telephone payments system from Content Guru called Storm.

4.3.3 Calls must not be transferred between the University's phone system and the dedicated telephone payments system. The caller must be asked to call directly to the dedicated telephone payments number.

5. Refunds

5.1 Any refund must be approved by an authorised signatory for the cost centre. The appropriate system is accessed and the refund should be processed back to the source card from which the original transaction was authorised.

5.2 If a transaction is older than 180 days, it may not be possible to be processed on to the source card for the original transaction. This is due to security measures implemented by the Payment Service Provider (PSP). In this instance, the customer should be contacted for their bank details so that the refund can be processed by BACS.

5.3 Business areas are reminded that refunds for face-to-face payments should not be carried out on our VoIP phone system. If the customer cannot be present in person with their card, they should provide their bank details so that the refund can be processed by BACS.

6 Access to sensitive cardholder data

6.1 All access to sensitive cardholder data must be controlled and authorised.

6.2 Any job functions that require access to cardholder data must be clearly defined.

6.3 Access to sensitive cardholder information such as PAN's, personal information and business data must be restricted to employees that have a legitimate business need to view such information.

6.4 A list of staff with a business need to access to the merchant copy will be maintained in each business area.

6.5 Only authorised employees should have access to this confidential data.

6.6 If cardholder data is shared with a Service Provider (3rd party) then a list of such Service Providers will be maintained by the PCI DSS Compliance Group.

6.7 The University will ensure that there is a written agreement, which includes an acknowledgement that the Service Provider will be responsible for the cardholder data that the Service Provider processes.

6.8 The University will ensure that there is an established process, including proper due diligence, in place before engaging with a Service Provider.

6.9 The University will have a process in place to monitor the PCI DSS compliance status of the Service provider.

6.10 Photocopies of credit cards should never be taken or stored.

7 Physical Security

7.1 Access to sensitive information in both hard and soft copy must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.

7.2 Employees must take all necessary steps to prevent unauthorized access to confidential data, which includes card holder data.

7.3 A list of devices that accept payment card data should be maintained:

- The list must include the make, model and location of the device;
- The list must have the serial number or a unique identifier of the device; and
- The list must be updated when devices are added, removed or relocated.

7.4 The surfaces of PED devices must be regularly inspected to detect tampering or substitution.

7.5 Personnel using the devices must be trained and aware of the correct handling the PED devices.

7.6 Personnel using the devices must verify the identity of any third-party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices.

7.7 Personnel using the devices must be trained to report suspicious behaviour and indications of tampering of the devices to the appropriate personnel.

7.8 A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.

7.9 Media is defined as any printed or handwritten paper, and/or received faxes.

7.10 Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals.

7.11 Visitors must always be escorted by a trusted employee when in areas that hold sensitive cardholder information.

7.12 Procedures must be in place to help all personnel easily distinguish between staff members and visitors, especially in areas where cardholder data is accessible. “Staff member” refers to full-time and part-time employees, temporary personnel, and consultants who are “resident” on University sites.

7.13 All PED devices must be appropriately protected and secured so they cannot be tampered or altered.

7.14 Strict control must be maintained over the external or internal distribution of any media containing card holder data and has to be approved by management.

7.15 As outlined previously, strict control must be maintained over the storage and accessibility of media containing sensitive cardholder information.

7.16 <u>It is strictly prohibited to store:</u>

- The contents of the payment card magnetic stripe (track data) on any media whatsoever.
- The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever.
- The PIN or the encrypted PIN Block under any circumstance.
- This data must never be collected over the telephone. Telephone payments must always be taken on the Storm system, the designated system for secure telephone payments.

8. Compliance and Monitoring

8.1 All card processing activities of the University must comply with PCI DSS. No activity or technology may obstruct compliance with the PCI DSS.

8.2 All Business Areas must adhere to this Policy to minimise the risk to both Customers and the University. Failure to comply will render the University liable for fines and may also result in Visa and/or MasterCard preventing transactions from being processed by the University.

8.3 Compliance with PCI DSS will be monitored through annual Self-Assessment Questionnaire (SAQ) returns. The PCI DSS Compliance Group will make returns on PCI DSS compliance to the University's Merchant Bank or their appointee when required.

8.4 Through meetings with relevant staff, the PCI DSS Compliance Group will conduct regular checks that identify threats, and vulnerabilities, and result in a formal risk assessment.

8.5 The University may screen potential employees to minimize the risk of attacks from internal sources.

8.6 The University will contractually require all third-parties with access to cardholder data to adhere to PCI DSS requirements. These contracts will clearly define information security responsibilities for contractors. The University will also contractually pass responsibility for data protection where personal data is passed to a third party for processing.

8.7 If staff have difficulties implementing or complying with any aspect of this policy, they should contact a member of the PCI DSS Compliance Group.

9 Responsibilities

9.1 Finance

The Finance Directorate has ultimate responsibility for PCI DSS compliance and will be responsible for the following:

- Promoting the policy and its ongoing application and adherence across the University;
- Providing training and awareness to all relevant staff;
- Working with Faculties and Directorates to ensure compliance through regular assessments and to provide support to address any gaps;
- Delegating authority for the approval of the use of Chip & PIN machines to a single member of the PCI DSS Compliance Group;
- Annual review of Incident Response Plan;
- Verifying the credentials/certification and maintaining records of whether a third-party provider has or does not have the necessary qualification to provide the appropriate PCI DSS processing services; and
- Maintaining an up-to-date list of all payment devices and users.

9.2 Digital & Information Services

The Digital & Information Services Directorate will be responsible for providing the following:

- Technical guidance necessary to assess and implement card processing solutions that are PCI DSS compliant;
- The necessary technical support to implementation of this policy;
- Assisting in the promotion of the Policy and in its ongoing application and adherence across the commercial units within the University;
- Lead on completion of the annual revalidation questionnaires;

- Maintain the Incident Response Plan;
- Assistance with the verification of the credentials/certification and maintaining records of third-party provider(s); and
- The necessary information governance support in this area.

9.3 Heads of School/Directors and card data business process owners

Heads of School/Directors and card data business process owners will be responsible for the following:

- Ensuring that their School or Directorate complies with this policy;
- Where there are gaps in the application of the policy, that these are brought to the attention of the PCI DSS Compliance Group;
- Engaging with the PCI DSS User Group forum; and
- Working with Finance and/or Digital & Information Services to implement any measures required to secure ongoing compliance with this policy.

9.4 PCI DSS Groups

A PCI DSS Compliance Group, comprising members of the Finance, Digital and Information Services, Student & Campus Life Directorates, Alumni Engagement and Philanthropy and the Information & Compliance Office will be responsible for ensuring annual compliance with the PCI DSS and ongoing adherence to the payment security policy.

A wider PCI DSS User Group, supported by the Finance Directorate, includes relevant stakeholders and representation from the PCI DSS Compliance Group.

10 Review

This policy will be reviewed on an annual basis. Any significant change to the PCI DSS or University policy or procedures, primarily concerned with information confidentiality, integrity and accessibility, may trigger an earlier review. This policy will be presented to the University Operating Board for initial approval, and then reviewed, thereafter, by the Finance Digital Committee. Any changes to the policy will be communicated to Finance Directorate Management Team to note.

11 Sanctions

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

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

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

Where contractual terms have been broken the University will review its position with that party. This could lead to termination of a contract of employment, studies, research or the provision of goods/services. Where it is believed that a criminal action has occurred, the University will also enact its Fraud policy.

12 Availability

This policy will be published on the University intranet.

13 Points of Contact

PCI DSS Compliance Group Teams site – PCI DSS Compliance Group
Cyber Security Manager – cybersecurity@qub.ac.uk
Head of Student Finance – Studentfinance@qub.ac.uk
Information Compliance Unit – Info.compliance@qub.ac.uk

14 Glossary of Terms

	Explanation
Acquirer	Also referred to as 'merchant bank'. This is the entity which initiates and maintains relationships with merchants for the acceptance of payment cards. In the case of the University, this is Worldpay.
Card Verification Code	Also known as Card Validation Code or Value, or Card Security Code. Refers to either: (1) magnetic-stripe data, or (2) printed security features. 1. Data element on a card's magnetic stripe that uses secure cryptographic processes to protect data integrity on the stripe, and reveals any alteration or counterfeiting. Referred to as CAV, CVC, CVV, or CSC depending on payment card brand. The following list provides the terms for each card brand: • CAV – Card Authentication Value (JCB payment cards) • CVC – Card Validation Code (Mastercard payment cards) • CVV – Card Verification Value (Visa and Discover payment cards) • CSC – Card Security Code (American Express)
EMV	**EMV** stands for Europay, MasterCard, and Visa, the three companies which originally created the standard. The standard is now managed by EMVCo, a consortium with control split equally among Visa, Mastercard, JCB, American Express, China UnionPay, and Discover.
Merchant Bank	For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, Mastercard or Visa) as payment for goods and/or services. Note that a merchant that accepts payments cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers. In the case of the University, the Merchant Bank is currently Worldpay.
P2PE	P2PE (point-to-point encryption) is a security standard that requires credit card information to be encrypted instantly upon

	its initial swipe and then securely transferred directly to the payment processor before it can be decrypted and processed.
PCI DSS	Acronym for “Payment Card Industry Data Security Standard”
PCI SSC	Acronym for “Payment Card Industry Security Standards Council”
PA-DSS	Acronym for “Payment Application Data Security Standard”.
Payment Cards	For purposes of PCI DSS, any payment card/device that bears the logo of the founding members of PCI SSC, which are American Express, Discover Financial Services, JCB International, Mastercard, or Visa, inc
PSP	Payment Service Provider (In the case of the University, this relates currently to Worldpay, Blackbaud and Shopify)
PED	PIN Entry Device (credit card terminal)
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 user and the particular cardholder account.
POS	Acronym for “point for sale”. Hardware and/or software used to process payment card transactions at merchant locations.
PIN	Acronym for “personal identification number”. Secret numeric password known only to the user and a system to authenticate the user to the system. The user is only granted access if the PIN the user provided, matches the PIN in the system. Typical PINs are used for automated teller machines for cash advance transactions. Another type of PIN is one used in EMV chip cards where the PIN replaces the cardholder’s signature.
Risk Analysis/Risk Assessment	Process that identifies valuable system resources and threats; quantifies loss exposures (that is, loss potential) based on estimated frequencies and costs of occurrence; and (optionally) recommends how to allocate resources to countermeasures so as to minimise total exposure.
SAQ	Acronym for “Self-Assessment Questionnaire”. Reporting tool used to document self-assessment results from an entity’s PCI DSS assessment.
Service Provider	Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. If an entity provides a service that involves only the provision of public network access – such as a telecommunications company providing just the communication link – the entity would not be considered a service provider for that service (although they may be considered a service provider for other services).
VoIP	Voice over Internet Protocol, also called IP telephony, is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol networks, such as the Internet. The terms Internet telephony, broadband telephony, and broadband phone service specifically refer to the provisioning of communications services over the public Internet, rather than via the public switched telephone network.
Virtual Payment Terminal	A virtual payment terminal is a web-based access to an acquirer, processor or third party service provider website to authorise payment card transactions, where the merchant manually enters payment card data via a securely connected web browser.

	Unlike physical terminals, virtual payment terminals do not read data directly from a payment card. Because payment card transactions are entered manually, virtual payment terminals are typically used instead of physical terminals in merchant environments with low transaction volumes.