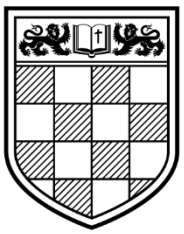

UNIVERSITY OF WINCHESTER

PCI-DSS CARDHOLDER DATA POLICY

Document Title:	PCI-DSS Cardholder Data Policy
Responsible Role and Department:	Director of Finance and Planning
Approving Body:	Executive Leadership Team (ELT)
Date of Approval:	15 July 2025
Date Effective From:	15 July 2025
Review Date:	01 March 2026
Indicate whether the document is for public access or internal access only. **Indicate whether the document applies to collaborative provision?** *(Strikethrough text, as appropriate)*	**Public Access** ~~**Internal Access Only**~~ **Applies to Collaborative Provision**

Summary:

This PCI-DSS Cardholder Data Policy is a sub-policy of the Information Security Policy and outlines the University's requirement to comply with PCI-DSS to process card payments. It is designed to ensure we can meet the standards required by the Payment Card Industry's Data Security Standard (PCI-DSS), which is a worldwide standard set up to help businesses (merchants) process card payments securely and reduce card fraud.

Contents **Page**

1. Scope

1.1 Everyone involved with handling credit and debit cards, credit and debit card data and the systems processing such data within the University of Winchester are subject to this policy.

1.2 This includes all members of the University (staff, students, and associates), members of other institutions who have been granted access to use the University's facilities, together with any others who may have been granted permission to use the University's information and communication technology facilities by the Director of Knowledge and Digital Services.

2. Definitions

2.1 The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organisations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover and JCB. The PCI Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. The standard was created to increase controls around cardholder data to reduce credit card fraud.

2.3 'Credit/Debit card data' or 'cardholder data' means most of the information on a credit card or debit card and includes the long 16-digit card number (Primary Account Number - PAN). It also includes the issue and expiry dates, the cardholder's name, the three-digit security code on the back of the card known as the Card Verification Value (CVV), any other information found on a card's magnetic stripe or chip, and any information relating to the card's PIN number.

3. What is PCI-DSS? (Payment Card Industry Data Security Standards)

3.1 The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards introduced by VISA, Mastercard and other payment brands that applies across the card payment industry worldwide. It helps safeguard cardholder information, improve customer confidence and reduce the risk of fraudulent transactions. These rules are compulsory for all organisations handling any aspect of card transactions who have access to cardholder data.

There are 12 requirements to PCI-DSS, these include:

Control Objectives	**Requirements**
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. Use and regularly update anti-virus software 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. Assign a unique ID to each person with computer access 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 all personnel

More information on PCI DSS can be located at https://www.pcisecuritystandards.org/ .

3.2 Card Payment Data

Card payment data consists of 2 main sets of data that must be protected by the University at all times. These include:

Cardholder Data	**Sensitive Authentication Data (SAD)**
Primary Account Number (PAN) i.e. the 16-digit number on the front of the card	Full Magnetic Stripe Data/Chip Data
Cardholder Name	CAV2/CVC2/CVV2/CID i.e. the last 3 digits on the signature strip on the back of the card
Expiration Date	Pin Numbers
Service Code	Pin Numbers
PCI DSS requirements are applicable if a primary account number (PAN) is stored, processed, or transmitted. If the PAN is not stored, processed, or transmitted, PCI DSS requirements do not apply	

4. Policy

4.1. Compliance and Requirements

Compliance with this policy is mandatory. Failure to follow this policy will be considered under the University's Disciplinary policy and may result in disciplinary action. A serious breach of the policy may constitute gross misconduct and lead to dismissal. Compliance with policies is primarily enforced through process and standard documents. Financial Services and Knowledge and Digital Services (KDS) will provide guidance and support but due to the diverse nature of the University's activities these processes and documents must be developed by each business area.

4.2. General

- Failure to protect card data can lead to large fines from the Information Commissioner's Office (ICO) and banks, expensive investigations, litigation, loss of reputation and in the worst-case scenario, withdrawal of the ability to take payment by debit and credit card, which would hinder the University of Winchester's ability to conduct business.

- No staff member should handle cardholder data unless they have a business need and explicit authorisation to do so.

- Cardholder data should only be handled in such a manner as is explicitly authorised by job roles.

- Electronic credit card data must not be transmitted by the University of Winchester via any private network that the University is responsible for unless in accordance with the handling requirements in this policy. This includes wired and wireless connections. Any card

processing devices such as tills and PDQ machines must be approved by Financial Services and KDS prior to connection to such network.

- University staff and students must not store credit and debit cardholder data on local hard drives, shared storage (such as University departmental file stores), cloud storage solutions (for example SharePoint), or any removable media (memory stick, CD/DVD) under any circumstances.

- Cardholder data must not be transmitted or requested to be transmitted via end-user messaging technologies such as email, instant messaging, or SMS. If unsolicited cardholder data is received via such means, this must be notified to the Information Compliance Officer and the data securely deleted.

- Any card data stored on University of Winchester systems must be reported to Knowledge and Digital Services immediately upon discovery by calling or raising a service desk ticket. It must be indelibly deleted from all devices, including any backups, at the earliest possible opportunity.

4.3. Credit/Debit Card Handling

It is the University's policy not to store cardholder data electronically or process that data on the University network. However, some processing of cardholder data will be carried out by the University on behalf of its staff and students. All processing of cardholder data must be approved by Financial Services and KDS and recorded in the faculty and professional services information asset registers and by Financial Services.

Any processing (including by third parties) must meet the following conditions:

- All handlers of cardholder data must be trained before being allowed access. This training must be recorded and repeated/updated upon hire and at least once every 12 months.

- Cardholder data must not be processed via digital connections provided by the University (wired or wireless). Where it is agreed that cardholder data can be directly processed by staff; public data networks (GPRS/3G/4G/5G) combined with strong encryption or properly configured P2PE solutions implemented in accordance with their respective Implementation Guides must be used instead. Analogue (telephone) lines are acceptable. Analogue telephone infrastructure must be properly secured against interference by unauthorised personnel.

- Cardholder data must not be stored in any voice recordings. Where cardholder data may be taken over the telephone, any call recording solution, including any Artificial Intelligence services which could "listen into" the data, must be disabled whilst cardholder data is being given.

- Any device used to process cardholder data on behalf of the University must be agreed to by Financial Services.
- For "Cardholder Not Present" transactions card information should only be entered into an electronic system (e.g. PDQ machine or computer application) and not written down (e.g. for later processing)

- Where the device is a Point-of-Sale (POS) terminal it must be of a type approved by Financial Services. The details (model, serial number, security features and location) of all examples in use must be recorded and supplied to Financial Services for inclusion in the asset list that they maintain. Such devices must be configured and used in accordance with Finance procedures.

- All devices must be stored securely when not in use and checked regularly for tampering or substitution. Any suspicion of tampering must be reported in line with the Incident response procedure.

- University staff and students must not store cardholder data on paper. The only exception is any paper output from compliant systems such as PDQ machines and tills as long as these have appropriate redaction. These should be kept for a stated retention period and then destroyed using a cross-cut shredder.

4.4. Third Parties

Any third party commissioned to handle cardholder information on behalf of the University of Winchester must be approved by Financial Services and Knowledge and Digital Services based on proper due diligence prior to engagement. Their compliance status must be assessed by the Information Compliance Officer.

If they are a PCI DSS compliant Service Provider for the contracted services they provide to the University, they will be required to provide the University with an up-to-date version of their Attestation of Compliance before engagement and each year thereafter.

Any contracts or written agreements with third party providers must make clear their responsibility for maintaining/protecting the University's compliance. A full list of Third-Party Payment Service Providers will be maintained by Financial Services, and the service providers PCI DSS compliance will be checked by Financial Services at least annually.

4.5. Incident Response

An Incident/Breach Response Plan must be in place, reviewed, and tested at least annually. Any breach or suspected breach must be reported immediately to Knowledge and Digital Services by calling or raising a ticket. This will be acknowledged shortly after receipt and escalated to the Incident Response group and Data Protection Team for further response.

4.6. Monitoring and Compliance Responsibilities

Overall responsibility for the University's PCI DSS compliance is held by the Chief Operating Officer (COO), as they are responsible for management of income, as well as the signatory of any contract with our acquirer/s. As the storage, transmission and processing of cardholder data and the associated risks are an Information Technology challenge, the Director of Knowledge & Digital Services also has a significant responsibility for ensuring adherence to this policy and associated procedures.

Any staff or students, including all permanent (direct hire), temporary and contract staff are responsible for ensuring our adherence with this policy. The Information Compliance Officer and the Director of Finance & Planning shall ensure it is available and promoted to those that need to see it.

It is the responsibility of the Director of Finance and Planning to maintain this policy and ensure it is reviewed at least triennially or if the environment changes. An assessment of the risks relating to the processing of cardholder data will be conducted annually by Financial Services with the support of Knowledge and Digital Services.

Knowledge and Digital Services, Information Compliance Team, Director of Finance & Planning, or any of their representatives, are authorised to inspect any systems, databases, or physical areas of the University where cardholder data might be processed or stored.

Many areas of the University 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 few Professional Services and Faculties.

All relevant Deans and Directors are responsible for ensuring that this policy is adhered to, that only University-approved devices and suppliers are used to receive payments, and that each MID has an identified and responsible manager. Financial Services are 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).

5. Further Guidance

The **Information Security Policy** can be found here

Appendix 1 University Approved Card Payment Methods and Services

Card data must only be received and processed by the University approved methods and services. These are:

Payment Method	Card Transaction	Mandatory Controls	Storage of Card Data
Customer NOT Present	**Online via University approved solution**	Payment via online system should generate an e-mail payment confirmation to the customer.	No Data is held by the approved University PCI-DSS compliant supplier
		If a customer's payment has been unsuccessful or declined, the customer should contact their card provider in the first instance.	
		If a customer faces difficult in making a payment then staff assistance can be provided.	
		If the payment problem cannot be resolved, the customer should be offered an alternative payment method.	
	Telephone	Where card details are provided during a telephone call, these must be processed directly into the PDQ terminal at that time. The card details must not be written down.	No Data is held by the approved University PCI-DSS compliant supplier
		When card details are being provided during a telephone call, these must not be repeated back to the customer in such a way that it can be intercepted by third parties.	
		If it is not possible to process the card details directly into the PDQ terminal immediately then a call back must be offered.	

Customer Present	**PDQ/EPOS** **Face-to-face transaction including contactless**	For contactless payments ensure the customer checks the value of the transaction before swiping their contactless card or device over the PDQ/EPOS terminal.	ONLY merchant receipts held in secure physical storage with PAN truncated and disposed of as confidential waste
		When the customer is present the card should be processed through the PDQ/EPOS terminal according to the on-screen instructions. Only the customer should handle their card unless you have to check a signature.	
		If the transaction is successfully processed, the merchant copy should be securely stored and the customer copy given to the customer.	
		If the transaction is declined, the customer should be advised immediately.	
		The customer copy stating that the payment was declined should be given to the customer and the merchant copy should be stored securely.	
		The option of paying with a different card should be offered.	

Equality Impact Assessment	
Summary of process undertaken to determine equality impacts:	The University does not collect diversity information of cardholders due to the risk of identification of an individual, this assessment was undertaken on the basis of potential impacts because of a protected characteristic. The Director of Equalities was consulted in relation to this.
University Committee (name/ date) where equality impacts discussed (maybe Committee of approval, or another):	N/A
Identified equality impact(s) on colleagues and students (i.e. any specific impacts related to this policy that may cause disadvantage for people due to one or more particular protective characteristic)	
Protected Characteristic	Impact(s) identified and any action(s)/mitigation(s) to address these impact(s), as necessary.
Age	Age may have an impact because of unfamiliarity with some technical concepts. This is mitigated by the requirement for all users to be trained (section 4.3 – first bullet-point), and the easy reference chart at Appendix 1
Disability	Neurodivergent and sight impaired colleagues and students may find the detail in this document difficult to navigate because of its (necessary) technical content. This is mitigated by the requirement for all users to be trained (section 4.3 – first bullet-point), and the easy reference chart at Appendix 1
Gender Identity	There are no likely impacts
Marriage/Civil Partnership	There are no likely impacts
Pregnancy and Maternity	There are no likely impacts
Race (incl. nationality)	There are no likely impacts
Religion and Belief	There are no likely impacts
Sex	There are no likely impacts
Sexual Orientation	There are no likely impacts