



Information Security - PCI DSS Cardholder Policy

1. Introduction

This PCI-DSS Cardholder Data Policy form part of the College's information security environment and outlines the College's requirement to comply with PCIS 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.

2. Scope

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

This includes all members of the College (staff, students and associates), and any others who may have been granted permission to use the College's information and communication technology facilities.

3. Definitions

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.

'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 and the three-digit security code on the back of the card known as the Card Verification Value (CVV).

4. Compliance and Requirements

Compliance with this policy is mandatory. Failure to follow this policy will be considered under the College's conduct procedure and may result in disciplinary action. A serious breach of the policy may constitute gross misconduct and lead to dismissal. Please contact the Vice Principal – Finance for further guidance and support.

5. 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 credit card; which would hinder the College's ability to conduct business.
- No staff member or student should handle cardholder data unless they have a business and/or teaching and learning 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 shall not be transmitted by the College via any private network that the College is responsible for unless in accordance with the handling requirements in this policy. This

includes wired and wireless connections.

- College staff and students shall not store credit and debit cardholder data on local hard drives, shared storage (such as College networks), cloud storage solutions (for example SharePoint), or any removable media (memory stick, CD/DVD) under any circumstances.
- Cardholder data shall 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 Vice Principal - Finance and the data securely deleted.
- Any card data stored on the College's systems must be reported to the Vice Principal – Finance immediately upon discovery.

6. Credit/Debit Card Handling

It is the College's policy not to store cardholder data electronically or process that data on the College network. There will be however some processing of cardholder data done by the College on behalf of its staff and students. All processing of cardholder data must be agreed and recorded by IT Services and by the Vice Principal – Finance.

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 and at least once every 12 months.
- Cardholder data must not be processed via digital connections provided by the College (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 shall not be stored in any voice recordings. Where cardholder data may be taken over the telephone, any call recording solution shall be disabled whilst cardholder data is being given.
- Any device used to process cardholder data on behalf of the College must be first agreed by the Vice Principal - Finance.
- Where the device is a Point-of-Sale (POS) terminal it must be of a type approved by the Vice Principal - Finance. The details (model, serial number, security features and location) of all examples in use must be recorded and supplied to the Finance department 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.
- College staff and students must not store cardholder data on paper unless specifically agreed by the Vice Principal - Finance. Any cardholder data may only be stored on paper prior to authorisation of payment (not after). It must be securely stored when not in use and destroyed.

7. Third Parties

Any third party commissioned to handle cardholder information on behalf of the College must be approved by the Vice Principal - Finance based on proper due diligence prior to engagement. Their compliance status must be assessed by the Vice Principal - Finance. If they are a PCI DSS compliant Service Provider for the contracted services they provide to the College, they will be required to provide the College 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 College's compliance. A full list of Third Party Payment Service Providers will be maintained by the Finance department.

8. 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 the Vice Principal - Finance. This will be acknowledged shortly after receipt.

9. Monitoring and Compliance Responsibilities

Overall responsibility for the College's PCI DSS compliance is held by the Vice Principal - Finance, 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 largely an Information Technology challenge, the Director of Digital Innovation 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 Vice Principal - Finance shall ensure it is available and promoted to those that need to see it.

It is the responsibility of the Vice Principal - Finance to maintain this policy and ensure it is reviewed at least annually or if the environment changes. An assessment of the risks relating to the processing of cardholder data will be conducted annually by the Vice Principal - Finance.