South Gloucestershire & Stroud College

Payment Card Industry Data Security Standard (PCI DSS) - Cardholder Data Policy

If you would like this document in an alternate format

Please contact the Human Resources Department

Prepared by:	Rich Aitken
Job Title/Role:	Head of Finance
Ref. No.: Q/P 223	**Date of this version:** 26 January 2021 **Review date:** 26 January 2023 (Subject to any legislative changes) **Upload to College website?** No **Upload to e-Campus?** Yes
Approved by:	Group Exec
Date of Approval:	April 2021

PCI DSS - Cardholder Data Policy

1. Introduction

1.1. This policy is designed to ensure South Gloucestershire and Stroud College ("the College") 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. The College must comply with PCI DSS to process card payments.

2. Statement

2.1. This policy applies to everyone involved with handling credit and debit cards, credit and debit card data and the systems processing such data within the College.

3. Objectives

3.1. To provide management direction and support for cardholder data security in accordance with business requirements and relevant laws and regulations.

4. Definitions

4.1. 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.

4.2. 'Credit/Debit card' or 'cardholder' data means most of the information on a credit card or debit card and includes the 16-digit primary account number (PAN). It also includes the issue and expiry dates and the cardholder's name.

4.3. The three-digit security code on the back of the card is known as the Card Verification Value (CVV) or Card Verification Code (CVC).

5. Implementation

5.1. Compliance

5.1.1. Compliance with this policy is primarily enforced through process and standard documents. The Finance Department will provide guidance and support.

5.1.2. Where any contradictions arise within the handling of cardholder data between this and other College policies, this policy takes precedent.

5.2. Personnel Policy

5.2.1. Terms and Conditions

5.2.1.1. All employees involved with handling cardholder data must comply with this policy and all other information security policies of the College.

5.2.1.2. Any cardholder data security incidents resulting from non-compliance may result in appropriate disciplinary action.

5.2.1.3. If, after investigation, a user is found to have violated the College's PCI DSS - Cardholder Data Policy and/or procedures, they may be disciplined in line with the organisation's formal disciplinary process.

5.2.2. Training and Awareness

5.2.2.1. All handlers of cardholder data must be adequately screened and trained before being allowed access. This training must be recorded and repeated annually and updated regularly.

5.3. General

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

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

5.3.3. College staff shall not store credit and debit cardholder data on local drives, shared storage, cloud storage solutions, or any removable media (memory stick, CD/DVD) under any circumstances.

5.3.4. 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 IT Helpdesk and Finance Operations Manager and the data securely deleted.

5.3.5. Any cardholder data stored on College systems must be reported to Finance@sgscol.ac.uk immediately upon discovery.

5.4. Cardholder Data Handling

5.4.1. All processing of cardholder data must be agreed and recorded by the Finance Department.

5.4.2. 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.

5.4.3. Any device used to process cardholder data on behalf of the College must have prior approval from the Finance Department.

5.4.4. Where the device is a Point-of-Sale (POS) terminal it must be of a type approved by the Finance Department. The details (model, serial number, security features and location) of all examples in use must be recorded in an asset list maintained by the Finance Department.

5.4.5. POS devices must be configured and used in accordance with Finance procedures.

5.4.6. All devices must be stored securely when not in use and checked regularly for tampering or substitution. Any suspicion of tampering must be immediately reported to the Finance Operations Manager or Head of Finance.

5.4.7. Staff must not store cardholder data on paper unless specifically agreed in advance by the Finance Operations Manager or Head of Finance. It must be securely stored when not in use and destroyed by placing in a locked confidential waste bin.

5.4.8. The full PAN must be masked on display, including on all merchant copy paper receipts, except for those business roles with a legitimate need to see more than the first 6 and last 4 digits.

5.5. Third Parties

5.5.1. Third parties commissioned to handle cardholder information on behalf of the College must be approved by the Finance Department based on proper due diligence prior to their engagement.

5.5.2. The compliance status of third parties must be assessed by the Finance Department and they will be required to provide the College with an up-to-date Attestation of Compliance before engagement and each year thereafter.

5.5.3. Any contracts or written agreements with third parties must make clear their responsibility for maintaining and protecting the College's compliance.

5.5.4. A list of Third-Party Payment Service Providers must be maintained by the Finance Department, and the service providers' PCI DSS compliance must be checked at least annually.

5.6. Incident Response

5.6.1. An Incident/Breach Response Plan must be in place, reviewed and tested at least annually.

5.6.2. Any breach or suspected breach must be reported immediately to Finance@sgscol.ac.uk who must subsequently notify the Data Protection Officer as well as IT Services if the breach is IT related.

6. Responsibilities

6.1. This policy is applicable to all staff (including temporary and contract), students and any other parties who may have access to cardholder data.

6.2. The Finance Operations Manager and the Head of Finance shall ensure the policy is available and promoted to those that need to see it.

6.3. Relevant Heads of Department shall be responsible for ensuring this policy is adhered to and that each POS terminal has an identified responsible manager.

6.4. The Finance Operations Manager shall be responsible for maintaining a register of Merchant IDs (MID) and assets in use relating to each MID (e.g. POS terminals).

7. Related Policies, Procedures, Code of Practice and Legislation

7.1. IT Security Policy

7.2. Data Privacy & Protection Policy

7.3. Disciplinary Procedures

NB This is not an exhaustive list. Other Policies, Procedures and Legislation may apply

8. MANDATORY INITIAL IMPACT SCREENING

Completed by:		
Name: Rich Aitken	Title: Head of Finance	26/01/2021
I have read the guidance document: Completing a Policy Impact Assessment?		✓
If this policy has been up-dated, please tick to confirm that the initial impact screening has also been reviewed:		☐

EQUALITY AND DIVERSITY IMPACT ASSESSMENT	
Characteristic	This policy seeks to:
Age	Choose an item.
Disability	Choose an item.
Faith or Belief	Choose an item.
Gender	Choose an item.
Race or Ethnicity	Choose an item.
Orientation	Choose an item.
Gender reassignment	Choose an item.
Economic disadvantage	Choose an item.
Rural isolation	Choose an item.
Marriage	Choose an item.
Pregnancy & maternity	Choose an item.
Carers & care leavers	Choose an item.
Vulnerable persons	Choose an item.
Please identify any sections of the policy that specifically seek to maximise opportunities to improve diversity within any of the College's stakeholder groups:	
Please identify any sections of the policy that specifically seek to improve equality of opportunity within any of the College's stakeholder groups:	

Is there any possibility that this policy could operate in a discriminatory way?	☐	×	If you have ticked yes (red), which characteristic will be most affected? Choose an item.
If yes please confirm that the Policy has been sent for a full Equality & Diversity Impact Assessment, and note the date:	☐		Click or tap to enter a date.

Note: if the policy does not seek to increase diversity or improve equality you should go back and review it before submitting it for approval.

MAPPING OF FUNDAMENTAL RIGHTS	
Which United Nations Convention on the Rights of the Child (UNCRC), Right does this policy most protect:	Choose an item. Choose an item. Choose an item.
Which Human Right (HRA) does this policy most protect:	Choose an item. Choose an item.

DATA PROTECTION & PRIVACY BY DESIGN SCREENING	
Tick to confirm that you have considered any data protection issues as part of the design and implementation of this policy; and, that implementing this policy will not result in the collection, storage or processing of personal data outside of official College systems:	✓
Tick to indicated that this policy has or requires a Data Privacy Impact Assessment:	☐