

PCI Compliance Policy

Adopted by Board: 16 March 2021

Review Period: 3yr

Review Date: March 2024

Person responsible for policy: Chief Financial Officer

**BePART Educational Trust Compliance policy is:**

* BePART Educational Trust (“The Trust”) will undertake a PCI Compliance review on an annual basis.
* If any member of staff identifies that this policy is compromised or is at risk of compromise then he/she must report the matter immediately to the Chief Financial Officer (“CFO”).
* All staff who handle either “Customer present” or “customer not present” card transactions in any form shall undertake PCI Compliance training on an annual basis.
* All “customer present” card transactions must take place using a secure PCI compliant electronic point of sale system.
* Where an electronic point of sale system is hired for an ad-hoc event, it must be both fully PCI Compliant and operate in PCI Compliant environment.
* Wherever possible “customer not present” card transactions should be processed using the Trust’s approved payment gateways.
* Where a personal computer or similar is used to access systems to process card transactions, the personal computer or similar must be an asset of the Trust. A personal computer owned by an individual must not be used.
* Under no circumstances should card and/or cardholder details be stored or transmitted electronically (other than through the Trust’s online store or PCI approved gateway). This includes emailing, instant messaging, chat and scanning of paper copies.
* If there is a valid requirement to scan paper copies containing card transaction details, the card details must be obliterated using an indelible marker pen before scanning.
* Where paper copies containing card transaction details need to be retained for a valid reason, for example chargebacks, they must be retained in a secure, locked cabinet or room at all times.
* The retention period for all paper copies containing card transaction details is:
	+ File by date of transaction
	+ Merchant copies should be kept for a minimum of 6 months (this is the time limit with which chargebacks can be registered).
	+ Beyond this, copies should be kept for a further 12 months *(i.e. total storage time equals 18 months from date of transaction)*
* All other paper copies containing card transaction details must be destroyed (cross shredded) immediately after use.
* The Trust will carry out security penetration testing annually on the Trust network and the results will be notified to the CFO.
* The Trust will use and regularly update anti-virus software to protect the Trust network and its personal computers that are connected to the card payment process.
* The Trust will contract an approved external supplier to carry out quarterly vulnerability scans of the relevant Trust IP addresses that are linked to the card payment processes and the results will be notified to the CFO.
* All individuals handling card data are expected to comply with Financial Regulations

**PCI Data Security Policy**

* Introduction

This policy provides essential information for everyone tasked with handling credit and debit cards, credit and debit card data and the systems processing such data within the Trust. It is designed to ensure we can meet the standards required by the Payment Card Industry’s Data Security Standard (PCI-DSS), which the Trust is obliged to meet in order to be able to process credit card payments.

* Scope

All environments within the Trust where credit and debit cards are handled. This environment is defined as the “Cardholder Environment” (“CDE).”

* Compliance Requirements

Compliance with this policy is mandatory. Failure to follow this policy can expose the Trust to financial penalties and operational risks.

* Definitions

‘Cardholder data’ refers to any information linked to a credit or debit card. This may include the name and address of the cardholder and/or any of the PAN, CVV, and issue or expiry date of the card.

‘PAN’ or Primary Account Number. This is the long 16 digit card number at the front of a debit or credit card.

‘CVV’ or Card Verification Value. This is the three digit security code on the back of most credit or debit cards.

**General**

* System users shall not send cardholder data unencrypted, via end-user messaging technologies such as, e-mail, instant messaging or chat without using an approved encryption solution. Where a solution is not available the data shall not be sent via any of these methods.
* Users shall not store cardholder data on local hard drives or other external or mobile media. If anyone must store confidential data on a hard disk that is not in a securely protected environment, they must report this to John Paul Szkudlapski, Senior Director of IT Services so that an appropriate security solution can be implemented.
* All employees, third parties or contractors are responsible for the Trust assets, particularly confidential data that they use to carry out their function. Any suspicious activity or suspect breach in security must be immediately report to John Paul Szkudlapski, Senior Director of IT Services.
* All documents containing cardholder data should be securely locked away after use.

**Credit and Debit Card Handling**

Scope

This section provides the minimum mandatory requirements that need to be applied to all employees who handle or come across cardholder data, in any format within the Trust environment. Furthermore any third party that uses or accesses any of the Trust’s cardholder data, either physically or logically, must also comply with this section. The Trust does not intend to electronically hold or store cardholder data, however, this section outlines what to do if such a situation arises.

**Policy Statements**

General

* Failure to protect card data could lead to significant ramifications for the Trust and could greatly hinder the Trust’s ability to conduct business. Failure to protect cardholder data can also be considered a breach of the Data Protection Act 2018 and any subsequent amendment or replacement to this legislation.
* No member of staff should handle cardholder data unless they have been trained and are authorised to do so.

Cardholder Data Requirements

* The PAN must always be encrypted when electronically stored and any other cardholder data, if stored with the PAN must be protected.  The Network and Security Services Manager can advise on a suitable encryption solution.
* The CVV should be handled with great care and should never be written down or stored anywhere. This includes written records in notes, on a form, database, spreadsheet or any other electronic format, even if encrypted. The only exception to this is where the CVV needs to be stored temporarily pre-authorisation whilst you arrange to take a payment. After a transaction has been authorised the CVV must be destroyed immediately.
* If during the performance of your job you can see, by error or intention, a full PAN when it is not required for you to do your job, please report this to the CFO. If however your job requires that you need access to the full PAN and you have not yet received training in PCI DSS then please report this to your line manager so that they can help arrange training.

Cardholder Data Handling Requirements

* Cardholder data should NOT be stored unless otherwise approved by the CFO.
* If you intend to store cardholder data you must inform the CFO.
* Do not store cardholder data on laptops, desktop computers, file shares, memory sticks or CDs unless these are on approved systems. If in doubt, do not store the data.
* Do not store cardholder data in spreadsheets and other office documents, unless:
* It is specifically required for your work;
* Storage has been approved in writing by the CFO; and
* The document is encrypted to AES-256 bit standard.
* Any cardholder data found on Trust systems must be reported to the CFO immediately upon discovery.

Printing of Documents Containing Cardholder Data

* At no point should cardholder data be printed without prior approval from CFO. Printing may involve cardholder data being sent across Trust networks in a manner that fails to meet PCI DSS requirements.

Handling Documents Containing Cardholder Data

* There are numerous cases where cardholder data can be legitimately stored on paper e.g. a chargeback letter, fraud document, an exceptions report etc. This data needs to be retained only until data can be processed electronically.

Vigilance and Awareness

* Each employee or contractor is responsible for the protection of the Trust’s assets which include all forms of data. It is therefore important that, should you see any cardholder data or other confidential data in a place that is insecure, inappropriate or where you do not expect to see it, you must secure the data, e.g. lock it in your desk and report it to the CFO

**PCI-DSS Cardholder Data Management**

Scope

This section provides the minimum mandatory requirements that need to be applied to all data created, transmitted, stored or managed by Trust within the CDE; be that data in hard (e.g. paper) or electronic (e.g. hard disk) formats. Furthermore any third party that uses or accesses any of Trust’s data within the CDE, either physically or logically, must also comply with this policy.

**Statements**

Data Protection Policy

The Trust Data Protection Policy sets out how the Trust collects, stores and processes personal data including the security and management of that data. All Trust staff, students and other authorised third parties, who have access to any personal data held by or on behalf of the Trust, must adhere to the Trust’s Data Protection Policy and associated Codes of Practice.

The Trust's Data Protection Officer handles day-to-day issues relating to notification, advice on compliance and responding to requests from data subjects.

* Breaches of the data protection legislation may lead to severe financial or reputational damage to the Trust.
* Cardholder data shall not be copied or transmitted in any format without the prior permission of the cardholder. All cardholder data in the CDE should be encrypted when stored electronically. John Paul Szkudlapski, Senior Director of IT Services should be contacted for any queries regarding encryption.
* All confidential data in the CDE must be handled in accordance with the data protection legislation, the Trust Data Protection Policy and associated Codes of Practice.

PCI-DSS Data Retention

* Cardholder data must not be retained on any Trust system.
* Other data referring to the cardholder data environment will be treated as outlined below:

**Payment Card Data**

Payment card data will not be stored within Trust.

**Revenue Protection Correspondence**

This refers to all correspondence relating to charge-backs, revenue protection and fraud prevention. These will typically be paper copies and must be destroyed by cross-cut shredding or approved shredding services once they have met their retention period.

**Information Systems and Physical Location Documentation**

All documentation relating to Information Systems within the PCI-DSS CDE, including network diagrams, firewall access, system configuration, system passwords and backup documentation must be held securely with privileged access.

Cardholder Data Security

Within the CDE:

* Cardholder data must not be sent to any external party without authorisation from the CFO and the cardholder, e.g. 2 separate people.
* All data physically sent to an external source must be sent via secure courier or other secure delivery method, as approved in advance by the data owner to ensure it is accurately tracked.
* All data must be stored in accordance with its classification regardless of the media it is held on.
* All physical backup media must be sent via secure transit.
* All data sent externally must be logged and those records retained for a period of 12 months.
* All physical (paper) and electronic confidential data, especially if it contains cardholder data, must have physical security controls applied at all times.
* All confidential data must be stored securely and all access to be secure and controlled based on a user’s “need to know”.
* Confidential data, especially cardholder data, stored on any form of media, e.g. CD’s, backups, hard drives, paper etc. must be inventoried to ensure the secure storage is managed and recorded.
* Periodic media inventories must be performed on a minimum of an annual basis. Evidence of media inventories will be retained.
* All confidential data, such as cardholder data, access passwords must be encrypted when stored. Stored data includes all logical locations, e.g. databases, servers, log files, debugging files, backups, reports etc.
* All system and application passwords are classified as confidential and need to be encrypted in all forms of transmission as well as in storage.

Cardholder Data Storage Locations

* The Trust does not electronically store cardholder data on its systems.

Cardholder Data Disposal

* The Trust should not hold any cardholder data.
* Should cardholder data exist on any system, the following conditions apply:
* All data must be securely disposed of when no longer required regardless of the media or application type on which it is stored.
* All hard copies of cardholder data must be manually destroyed as soon as it has reached the end of its retention period. A quarterly process must be in place to confirm that all non- electronic cardholder data has been appropriately disposed of in a timely manner.
* All hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed.

Mobile Data

* Cardholder data is not permitted to be stored on mobile devices.

**Responsibilities**

All users **within**the CDE include all permanent (direct hire), temporary and contract staff who use Trust computer systems. All users must use the IT systems, information and equipment in accordance with Trust security policies and procedures. Users are responsible for:

* Familiarising themselves with and adhering to the policies and procedures applicable to their area of responsibility;
* Clearing desks of all sensitive material and logging off or locking workstations at the end of the day and when leaving their desk;
* Not removing equipment, information or any other Trust property from the Trust premises without authorisation;
* Not connecting personal equipment to Trust networks within the CDE;
* Not installing, copying or modifying any software on Trust equipment without authorisation;
* Immediately reporting security incidents to John Paul Szkudlapski, Senior Director of IT Services

# Incident Reporting

**Incident Response Plan**

An “incident” is defined as a suspected or confirmed “data compromise”. A “data compromise” is any situation where there has been unauthorised access to a system or network where cardholder data is collected, processed, stored, or transmitted. For purposes of PCI DSS, a “data compromise” can also involve the suspected or confirmed loss or theft of any material or records that contain cardholder data.

 Some examples of data compromise incidents that an employee might recognise in their day to day activities include, but are not limited to:

* Theft, damage, or unauthorised access (e.g., papers missing from their desk, broken locks, missing log files, alert from a security guard, video evidence of a break-in or unscheduled/unauthorised physical entry)
* Fraud
* Inaccurate information within databases, logs, files or paper records
* Card terminals that have been tampered with or substituted
* Computers that have had a suspect device installed to the USB port

**Reporting an Incident**

* Employees are responsible for reporting incidents in their area to CFO who will report the incident to John Paul Szkudlapski, Senior Director of IT Services and any other relevant parties. If you become aware of a suspected or real security incident relating to cardholder data, or a failure in procedure, then you must act immediately.
* All communications with police or the public will be coordinated by the CFO.

**Incident Response**

The following measures must be immediately followed when a confirmed or suspected incident arises to ensure that a suspicious card terminal or computer cannot be used such as:

* Disconnecting the terminal’s network cable / telephone line (but DO NOT switch the device off);
* Put a note on the terminal stating that it is ‘not in use’;
* Keep a watchful eye over the device until further information is given.

Notify the CFO and John Paul Szkudlapski, Senior Director of IT Services of the confirmed or suspected incident by email, providing details or generalities surrounding the suspected or confirmed incident

Complete an Incident Response form (Appendix 1) and email to the CFO. The form should provide as much detail as possible, including the date, time, and the nature of the incident if known. Any information you can provide will aid in responding in an appropriate manner.

Responses may proceed through the following stages – this will be determined by the CFO:

* Alert all relevant parties, i.e. banking relationship manager, merchant/acquiring bank, police;
* Collect and protect information associated with the intrusion;
* In the event that forensic investigation is required, the CFO will work with legal representatives and management to identify appropriate forensic specialists;
* Eliminate the intruder's means of access and any related vulnerabilities;
* Research potential risks related to or damage caused by intrusion method used;
* Report to Directorate;
* Report to HEFCE;
* Report to the Information Commissioner.

**Post Incident Response**

 Not more than one week following the incident, the CFO and all affected parties will meet to review the results of any investigation to determine the root cause of the compromise and evaluate the effectiveness of the Incident Response Plan. Any identified areas in which the policy or security control can be made more effective or efficient, must be updated accordingly.

**Incident Response Plan Review**

It is required that this incident response plan be reviewed and tested annually and revised as needed.



**Incident Response form – Cardholder data breach**

**On completion, send to the officers recorded below\***

|  |  |  |
| --- | --- | --- |
| ***Requirement*** | **Response** | **CFO comments** |
| ***Note: The Data Protection Officer must be notified immediately and as a matter of urgency, of any potential incident or breach; this form is to be used to give more detailed information after it has been initially reported.*** |
| **Date/time of report** |  |  |
| **Name, job title and contact details of person writing report** |  |  |
| **Confirmed or Suspected Incident?** |  |  |
| **How did you become aware of the Incident?** |  |  |
| **Date/time of Incident (if known)** |  |  |
| **Nature of Incident** |  |  |
| **Areas / systems affected** |  |  |
| **Any other information surrounding the Incident?** |  |  |

|  |
| --- |
| **\* Reporting and decisions made** |
| **Name / Job Title reported to** | **Date reported** | **Decision of action to take** |
| CFO |  |  |
| Senior Director of IT Services |  |  |