Information Security Policy (PCI/DSS) (draft)

Policy number	New or Reviewed	Date of next review	Responsibility
P023	New November 2018	November 2020	IT Manager

To provide young people with opportunities to be
successful and make a positive contribution within their community.

Contents

1. Introduction

This Policy identifies the requirements of the Payment Card Industry Data Security Standard (PCI-DSS) at Fairfield Farm Trust. We use a range of technologies that enforce safer working practices across all areas of the business. This policy is intended for those involved in customer financial transactions via credit/debit card machines and those responsible for the management of this provision. This policy should be read in conjunction with Policy No. P017 e-safety and online protection policy (available in the Documents section of PeopleHR).
This Policy must be distributed to all employees who use credit/debit card machines. Employees must read this document in its entirety and be able to view it via the document section of our HR system 'PeopleHR'. It is required that they sign to say they understand this policy and know when to find it for reference or update purposes. This document will be reviewed and updated by the responsible person named on the coversheet of this document on an annual basis or when necessary to include newly developed credit/debit card security standards into the policy.

2. Ethics and Acceptable Use Policies

All College employees are required to conduct business in accordance with all applicable laws, regulations and contractual obligations. Employees must behave ethically, with integrity and adhere to all Company policies and procedures. It is the responsibility of the employee to be truthful, honest and co-operate fully with credit/debit card information security standards and regulations set out by FFT. In addition to this an employee must report inappropriate activity or unlawful conduct by another employee as outlined in Policy No. P008 Whistle blowing policy (available in the Documents section of PeopleHR).

Consumer confidence is of paramount importance to our charity and with this in mind FFT commits to respecting the privacy of all its customers and to protecting any data about them from unauthorised outside parties. To this end management are committed to maintaining a secure environment in which to process cardholder information so that we can meet these promises.

We use an end to end service provided by PaymentSense, this means we do not collect, store or hold any customer credit card details on our systems. Our IT systems are used as a means to transfer this encrypted data between the credit/debit card machines and the servers at PaymentSense however employees who are involved in payments made via credit cards should ensure:

- Cardholder information is protected and handled in a manner that fits with its sensitivity.
- Safe working practices are adhered to as stated in Policy No. P017 e-safety and online protection policy (available in the Documents section of PeopleHR).
- Information security incidents must be reported, without delay to the IT Manager or a member of SLT.

Furthermore as employees we each have a responsibility for ensuring our company's systems and data are protected from unauthorised access and improper use. It is imperative that employees understand the importance of safeguarding such sensitive information from third parties that do not need to have it to go about their daily business. Such information includes:

- Personal client information (name, address, telephone no., email address, driver's license no., bank account, credit card numbers etc.) and;
- Company information that is not readily available to the public (clients, financial information, employee information, schedules, technology etc.).

If you are unclear about any of the policies detailed herein you should seek advice and guidance from your line manager.

3. Disciplinary Action

Violation of the standards, policies and procedures presented in this document by any employee will result in disciplinary action as outline in the Employee Handbook (available in the Documents section of PeopleHR).

4. Protect Stored Data

As stated above FFT do not store any customer credit card details as part of collecting payment via its credit/debit card machines however to reinforce this it is strictly prohibited to store:

- 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.
- All digits of the credit card's primary account number on any media whatsoever. All digits but the last 4 numbers of the credit card account number must be concealed or masked (e.g. XXXX or ****) when the number needs to be displayed e.g on a till receipt.

5. Protect Data in Transit

All sensitive cardholder data must be protected securely if it is to be transported physically or electronically.

- Card holder data (PAN, track data etc.) must never be sent over the internet via email, instant chat or any other end user technologies.
- If there is a business justification to send cardholder data via email or via the internet or any other modes then it should be done after authorization and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, IPSEC, GSM, GPRS, Wireless technologies etc.).
- The transportation of media containing sensitive cardholder data to another location must be authorised by management, logged and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

6. Restrict Access to Data

Access to sensitive cardholder information such as PANS, personal information and business data is restricted to FFT employees that have a legitimate need to view such information. No other employees should have access to this confidential data unless they have a genuine business need, for further information see Policy No. P017 e-safety and online protection policy (available in the Documents section of PeopleHR).

7. Physical Security

Access to sensitive information in both hard and soft format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data. Media is defined as any printed or handwritten paper, USB flash drive, backup tapes, computer hard drive, etc.

- Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals.
- Media storing sensitive cardholder date (especially the PAN and other personal information such as national insurance numbers etc.) should be properly logged and inventoried before being destroyed. Sensitive data should always be disposed of when it is no longer needed by the FFT in such a manner as to render the content irrecoverable and to comply with GDPR regulations.
- Visitors must always be escorted by a trusted employee when in areas that hold sensitive cardholder information.
- All computers which store sensitive cardholder data must have a password protected screensaver enabled to prevent unauthorised use.
- Users are required to lock computers when leaving their desks etc. to prevent unauthorised use, for further details see Policy No. P017 e-safety and online protection policy (available in the Documents section of PeopleHR). A list of devices that accept credit/debit card data should be maintained by management.
    - The list should include make, model and location of the device
    - The list should have the serial number or a unique identifier of each device
    - The list should be updated when devices are added, removed or relocated
- POS devices surfaces should be periodically inspected to detect tampering or substitution.
- Employees using the devices should be trained and aware of handling the POS devices
- Employees using the devices should verify the identity of any third party personnel claiming to repair or

run maintenance tasks on the devices, install new devices or replace devices.

- Personnel using the devices should be trained to report suspicious behaviour and indications of tampering of the devices to the IT Manager or a member of SLT.

8. Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into the day-to-day practice of the FFT at both Executive and Departmental level to maintain a high level of security awareness. The protection of sensitive data demands regular updates to all employees and contractors.

1. Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day-to-day practice.
    - Distribute this policy document to all FFT employees to read and sign. It is a requirement of FFT that all employees involved with credit/debit card transactions confirm that they understand the content of this credit/debit card Information security policy by signing the acknowledgement slip at appendix 1.
    - All employees have to sign a user acceptable use policy (AUP) agreement attached to Policy No. P017 e-safety and online protection policy (available in the Documents section of PeopleHR) before any access is granted to FFT IT systems regardless of job role or circumstance.
    - All employees will undergo background checks (such as DBS) before they commence their employment with FFT.
2. All third parties with access to credit card account numbers are contractually obligated to comply with Card Association Security Standards (PCI/DSS).
3. FFT credit/debit card information security policies must be reviewed annually and updated as necessary.

9. Network Security

This section is required to comply with PCI/DSS regulations, it is not relevant for customer facing staff that deal with transactions via credit/debit card machines. It is relevant to the IT Manager and SLT.

Firewalls and network traffic

- Firewalls must be implemented at each internet connection, any demilitarized zone (DMZ) and the internal company network.
- A network diagram detailing all the inbound and outbound connections must be maintained and reviewed every 6 months by the IT Manager.
- A firewall and router configuration document must be maintained which includes a documented list of services, protocols and ports including a business justification.
- Firewall and router configurations must restrict connections between untrusted networks and any systems in the card holder data environment.
- Stateful Firewall technology must be implemented where the Internet enters FFT Card network to mitigate known and on-going threats. Firewalls must also be implemented to protect local network segments and the IT resources that attach to those segments such as the business network, and open network.
- All inbound and outbound traffic must be restricted to that which is required for the card holder data environment.
- All inbound network traffic is blocked by default, unless explicitly allowed and the restrictions have to be documented.
- All outbound traffic has to be authorised by management (i.e. what are the whitelisted category of sites that can be visited by the employees) and the restrictions have to be documented.
- FFT will have firewalls between any wireless networks and the cardholder data environment.
- FFT will provide relevant security for all wireless users, where they will be authenticated and firewalled so that they can't access unauthorised networks or in some cases each other i.e. guest access etc.
- Disclosure of private IP addresses to external entities must be authorized.
- A topology of the firewall environment has to be documented and has to be updated in accordance to the changes in the network.

- The firewall rules will be reviewed on a six months basis to ensure validity and the firewall has to have clean up rule at the bottom of the rule base.
- No direct connections from Internet to cardholder data environment will be permitted. All traffic has to traverse through a firewall and be encrypted.

Anti-virus

- All machines must be configured to run the latest anti-virus software as approved by FFT. The preferred application to use is '*Webroot secureanywhere endpoint protection'*, which must be configured to retrieve the latest updates to the antivirus program automatically on a daily basis. The antivirus should have periodic scanning enabled for all the systems.
- The antivirus software in use should be capable of detecting all known types of malicious software (Viruses, Trojans, adware, spyware, worms and rootkits).
- All removable media (for example floppy and others) should be scanned for viruses before being used.
- All the logs generated from the antivirus solutions have to be retained as per legal/regulatory/contractual requirements or at a minimum of PCI DSS version 3.2 requirement 10.7 of 3 months online and 1 year offline.
- Master Installations of the Antivirus software should be setup for automatic updates and periodic scans.
- End users must not be able to modify any settings or alter the antivirus software.
- E-mail with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any e-mail, which they suspect may contain virus.

Remote Access

- It is the responsibility of FFT employees, contractors, vendors and agents with remote access privileges to FFT's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to FFT.
- Secure remote access must be strictly controlled. Control will be enforced by two factor authentication via one-time password authentication or public/private keys with strong pass-phrases.
- Vendor accounts with access to FFT network will only be enabled during the time period the access is required and will be disabled or removed once access is no longer required.
- Remote access connection will be setup to be disconnected automatically after 30 minutes of inactivity.
- All hosts that are connected to FFT internal networks via remote access technologies will be monitored on a regular basis.
- All remote access accounts used by vendors or 3rd parties will be reconciled at regular interviews and the accounts will be revoked if there is no further business justification.
- Vendor accounts with access to FFT network will only be enabled during the time period the access is required and will be disabled or removed once access is no longer required.

Vulnerability Management Policy

As part of the PCI-DSS Compliance requirements, FFT will run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).

- All vulnerabilities found in scans detailed below (internal and external) will be assigned a risk ranking such as High, Medium and Low based on industry best practices.
- Quarterly internal vulnerability scans must be performed by FFT internal staff or a 3rd party vendor and the scan process has to include that rescans will be done until passing results are obtained, or all High vulnerabilities as defined in PCI DSS version 3.2 section 6.2 are resolved.
- Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by PCI SSC. Scans conducted after network changes may be performed by FFT's internal staff. The scan process should include re-scans until passing results are obtained.

10. Security Management / Incident Response Plan

Employees of FFT will be expected to report to the **GDPR Data Protection Officer (DPO)**, any security related issues. HR Department will effectively communicate and monitor electronic security policies and procedures to employees via our online HR System 'PeopleHR'. Contractors are expected to have signed a GDPR statement - see Policy No. 039 Data protection (GDPR) policy (available in the Documents section of PeopleHR) prior to any 'sensitive' data being shared. In addition, **DPO** will oversee the monitoring of information security updates outlined in both this document and oversee the implementation of the incident response plan in the event of a sensitive data compromise.

11. In the event of a suspected security breach, employees should:

- Alert **DPO** immediately who will carry out an initial investigation of the suspected security breach.
- Upon confirmation that a security breach has occurred, **DPO** will arrange for all relevant parties to be alerted that may be affected by the compromise.

If the security breach involves credit/debit card account numbers, **DPO** will implement the following procedure:

- Alert **IT Manager** to shut down any systems or processes involved in the breach to limit the extent, and prevent further exposure.
- Alert **Senior Finance Manager** to contact all affected parties and authorities such as the merchant Bank, card issuer (if known), MasterCard UK or VISA UK and any necessary law enforcement.
- **Senior Finance Manager** must provide details of all compromised or potentially compromised card numbers to either the card issuer (if known), MasterCard UK or Visa UK within 24 hours, for more information visit: MasterCard UK Safety Benefits or Visa UK Protection Benefits.

By order of the Board

Richard Wiltshire
IT Manager
November 2018

12. Appendix 1 – User Agreement

AGREEMENT TO COMPLY WITH THE INFORMATION SECURITY POLICY (PCI/DSS)

I understand that this policy requires a digital signature in 'PeopleHR' and that by signing it I am agreeing to the following points.

- I am able to find, download and read a copy of this policy from the Documents section of PeopleHR. I have read and understood the policy. I understand how it impacts on my role and as a condition of my employment, I agree to abide by the policy.

- I agree to take all reasonable precautions to assure that FFT credit/debit card information, or information that has been entrusted to FFT by third parties such as customers, will not be disclosed to unauthorised persons.

- At the end of my employment or contract with FFT I agree to return all information to which I have had access as a result of my position.

- I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the manager who is the designated information owner or written permission from the senior leadership team (SLT).

- I understand that non-compliance could result in disciplinary as outlined in the Employee Handbook (available in the Documents section of PeopleHR).

- I further agree to promptly report all violations or suspected violations of this policy to the DPO, My line manager, SLT or the IT manager.