Normandy Community Shop and Café Ltd
Information Management Policy

## 1. **Policy statement**

Normandy Community Shop and Cafe Ltd, hereafter known as 'the Shop' is a registered society under the Co-operative and Community Benefit Societies Act 2014 and owned by its members, the majority of whom are residents of the village of Normandy. The Society operates from Shop and Cafe site within Normandy village, in the foothills of the Surrey Hills for its residents and visitors to the area. The Shop is a socially responsible business committed to commercial success whilst upholding the highest standards with regards to business operations. This policy forms part of those standards of good practice.

This Information Security Policy:

- Defines the IT and Information Security Policy for the shop.
- Sets out the shop's high-level requirements for the management of Information Security in relation to the storage, processing and transmission of confidential data.
- Meets the compliance obligations to the Payment Card Industry Data Security Standard (the PCI DSS).Version 3.2, released in April 2016, in particular the standards for merchants with payment application systems connected to the Internet, no electronic cardholder data storage (SAQ C).
- Is compliant with the General Data Protection Regulation and the Data Protection Bill.

This policy should be read in conjunction with the Shop Data Protection Policy.

## 2. **IT and Information Security Policy**

### 2.1 **Purpose**

This document details the IT security strategy for the shop in relation to the storage, processing and transmission of confidential data including credit card data. Its aim is to set out the Information Security responsibilities for staff, contractors, partners and third parties.

As part of the shop's Payment Card Industry (PCI) Compliance programme, consideration has been made to Credit Card Processing operations. Guidelines and controls form an essential part of the shop's compliance status against the PCI Data Security Standard.

This document should be reviewed:

- At least annually when the shop undertakes its annual PCI compliance review.
- If any new credit card processing or IT systems or processes are implemented.

### 1.2 **Introduction**

Normandy Community Shop and Café Ltd handles sensitive cardholder information daily. Sensitive Information must have adequate safeguards in place to protect them, to protect cardholder privacy, to ensure compliance with various regulations and to guard the future of the organisation.

Normandy Community Shop and Café Ltd commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end the Society is committed to maintaining a secure environment in which to process cardholder and other confidential information so that we can meet these promises.

Normandy Community Shop and Café only uses standalone card readers and does not store any cardholder data electronically. All paper transaction records are stored in line with the Societies' Data Protection policy.

Access to Confidential information is limited to people whose role responsibilities require it.
All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS).

2.2 **Roles and Responsibilities**

The Board will identify a lead person, with responsibility for ensuring that the aims set out in this policy document are observed and monitored, together with the reviewing this policy. The shop IT Security lead may be:

- One of the Directors, who will be provided with appropriate training if required
- A designated manager, again, with training if required
- An IT Security specialist appointed by the Board

The shop IT Security lead is responsible for:

- Overall responsibility for Information Security and related issues.
- Development and maintenance of Information Security Policies and Procedures
- Communication and review of Information Security Policies.
- Coordination of PCI Security Audit Tasks.
- Coordination with PCI Accredited Security Auditors (Qualified Security Assessors (QSAs) and Approved Scanning Vendors (ASVs))
- Keeping the Board updated on all security related issues.

The Shop management team are responsible for ensuring that the requirements of this policy are adhered to, including responsibility for:

- Ensuring that staff are aware of the IT Security policies and procedures.
- Ensuring that the requirements of the IT Security policies and procedures within their control are adhered to.
- Reporting IT Security incidents or concerns to the IT Security lead and participating in implementing actions where required.

Staff and Shop Management with access to confidential and sensitive information must:

- Handle confidential and sensitive information in a manner that fits with their sensitivity.
- Protect sensitive information;
- Keep passwords and accounts secure;
- Not disclose personnel or confidential information unless authorised;
- Use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
- Report information security incidents without delay.

2.3 **Breaches of this policy**

The shop is committed to ensuring that our IT Security policy is effectively implemented. Any breaches of this policy coming to the attention of management and/or directors will be dealt with appropriately.

### 2.4 **Acceptable Use Policy**

• Staff are responsible for exercising good judgment regarding the reasonableness of personal use.
• Postings by employees from a shop email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Normandy Community Shop and Cafe Ltd, unless posting is during business duties.

### 2.5 **Access to the sensitive cardholder data**

• All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS).
• If cardholder data is shared with a Service Provider (3rd party) then a list of such Service Providers will be maintained as detailed in Appendix B.
• Normandy Community Shop and Café Ltd will ensure a written agreement that includes an acknowledgement is in place that the Service Provider will be responsible for the cardholder data that the Service Provider possess.
• Normandy Community Shop and Café Ltd will undertake appropriate due diligence before engaging with a Service provider.

### 2.6 **Physical Security**

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.

• Card reader devices should be appropriately protected and secured so they cannot be tampered or altered.
• Card reader devices surfaces should be periodically inspected to detect tampering or substitution.
• Staff 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.
• Media is defined as any printed or handwritten paper, memory sticks, CD-ROMS, etc.
• Strict control is maintained over the storage and accessibility of media

### 2.7 **Data in Transit**

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

• Card holder data (PAN, track data etc.) must never be sent over the internet via email, instant chat or any other end user technologies.
• The transportation of media containing sensitive cardholder data must be logged. Only secure courier services or other delivery method that can be tracked may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered.

### 2.8 **Disposal of Stored Data**

• 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 when no longer required for valid and justified business reasons. An annual 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 will be destroyed by shredding or incineration so they cannot be reconstructed.

2.9 **Network security**

• The network installed in the Shop will be segregated into a secure business network and a public network.

2.10 **Anti-virus and patch management**

• All machines must be configured to run the latest anti-virus software.
• All removable media (for example floppy and others) should be scanned for viruses before being used.
• 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.
• All Workstations, servers, software, system components etc. must have up-to-date system security patches installed to protect the asset from known vulnerabilities.
• Wherever possible all systems, software must have automatic updates enabled for system patches released from their respective vendors.

2.11 **IT Security Audits**

• Regular audits of IT Security will be undertaken, in line with the requirements of the PCI standards, and other standards, as appropriate.
• As part of the PCI-DSS Compliance requirements, Normandy Community Shop and Café Ltd will run the Cardholder Data Scan and any other scan required by PCI-DSS at least quarterly and after any significant change in the network

2.12 **Incident Response Plan**

The actions to be taken in response to a security incident are detailed in the Shop Business Continuity and Critical Incident plan

WIFI access is provided via an external provider which provide a secure login process and separates the business WiFi from the guest WiFi.