North Petherton Rugby Football Club LTD

Affiliated to the Rugby Football Union and the Somerset County Rugby Football Union

CASC REG. 04941

Information Security Policy – Payment via Credit Cards

Purpose

This Policy document encompasses all aspects of security surrounding confidential Club information and must be distributed to all staff members that are involved in the payment for goods via the operation of a credit / debit card hand-held machine. These staff members must read this document in its entirety and sign the form confirming they have read and fully understand this policy. This document will be reviewed and updated by the Information Security Officer on an annual basis or when relevant to include newly developed security standards into the policy and re-distributed to all staff where applicable

Scope

This policy gives guidance in relation to how North Petherton RFC handles sensitive cardholder information. NPRFC will have adequate safeguards in place to protect the cardholder's data, cardholder's privacy and to ensure compliance with various regulations.

Rationale

North Petherton RFC commits to respecting the privacy of all its customers and to protecting any customer data from outside parties. To this end the Club is committed to maintaining a secure environment in which to process cardholder information so that these promises can be met.

Procedure

NPRFC staff handling sensitive cardholder data should ensure that they:

- Handle cardholder information in a manner that fits with their job role and responsibility.
- Limit personal use of North Petherton RFC information and telecommunication systems.
- Do not disclose personnel information unless authorised;
- Protect sensitive cardholder information;
- Keep passwords and accounts secure;
- Request approval from the Information Security Officer prior to establishing any new software or hardware, third party connections, etc.;
- Do not install unauthorised software or hardware, including modems and wireless access unless they have explicit management approval;

- Information security incidents must be reported, without delay, to the Information Security Officer who is responsible for incident response.

All staff has a responsibility for ensuring the Club's systems and data are protected from unauthorised access and improper use. If further clarity is required about any of the policies detailed herein they should seek advice and guidance from the Information Security Officer.

Staff of NPRFC will be expected to report to the Information Security Officer for any security related issues. The role of the Information Security Officer is to effectively communicate all security policies and procedures to staff within the Club. In addition to this, the Information Security Officer will oversee the scheduling of security training sessions, monitor and enforce the security policies outlined in both this document and at the training sessions and finally, oversee the implantation of the incident response plan in the event of a sensitive data compromise.

Acceptable Use Policy

The Clubs Executive Committee is committed to protecting the Club and all its staff members from illegal or damaging actions, either knowingly or unknowingly by individuals. North Petherton RFC will maintain an approved list of technologies and devices and personnel with access to such devices as detailed in Appendix B.

- Staff that are listed in App B are responsible for exercising good judgment regarding the reasonableness of personal use.
- All staff listed, together with the Security Incident Response Team will take all necessary steps to prevent unauthorized access to confidential data which includes card holder data.
- Keep passwords secure. Authorized users are responsible for the security of the passwords involved when making contact with the service provider.
- All Point of Sale (POS) and Personal Identity Number (PIN) entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- The List of Devices in Appendix B will be regularly updated when devices are modified, added or decommissioned. A stock-take of devices will be regularly performed and devices inspected to identify any potential tampering or substitution of devices.
- Users should be trained in the ability to identify any suspicious behaviour where any tampering or substitution may be performed. Any suspicious behaviour will be reported accordingly.

Protect Stored Data

- All sensitive cardholder data stored and handled by North Petherton RFC and its registered staff members must be securely protected against unauthorised use at all times. Any sensitive card data that is no longer required by North Petherton RFC for business reasons must be discarded in a secure and irrecoverable manner.
- If there is no specific need to see the full PAN (Permanent Account Number), it has to be masked when displayed.

It is strictly prohibited to store:

1. **The contents of the payment card magnetic stripe (track data) on any media**

whatsoever.

2. **The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever.**
3. **The PIN or the encrypted PIN Block under any circumstance.**

Information Classification

Data and media containing data must always be labelled to indicate sensitivity level.

- **Confidential data** might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to North Petherton RFC if disclosed or modified. **Confidential data includes cardholder data**.

1. Access to the Sensitive Cardholder Data

All Access to sensitive cardholder data should be controlled and authorised. Any job functions that require access to cardholder data should be clearly defined.

- Any display of the card holder should be restricted at a minimum to the first 6 and the last 4 digits of the cardholder data.
- Access to sensitive cardholder information such as PAN's, personal information and business data is restricted to staff members that have a legitimate need to view such information.
- North Petherton RFC will adhere to an established process, including proper due diligence is in place, when engaging with a Service provider as described further in this policy

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.

- Media is defined as any printed or handwritten paper, device hard drive, etc.
- Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals.
- A list of devices that accept payment card data should be maintained.
- The list should include make, model and location of the device.
- The list should have the serial number or a unique identifier of the device
- The list should be updated when devices are added, removed or relocated
- POS devices surfaces are periodically inspected to detect tampering or substitution.
- Personnel using the devices should be trained and aware of handling the POS devices
- Personnel 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 Information Security Officer. Strict control is maintained over the external or internal distribution of any media containing card holder data and has to be approved by the Information Security Officer.
- Strict control is maintained over the storage and accessibility of media

Disposal of Stored Data

- All data must be securely disposed of when no longer required by North Petherton RFC, 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. North Petherton RFC will destroy all hardcopy (paper) materials. These will require that all hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed.

Security Awareness and Procedures

The procedures outlined below will be put into operation in order to maintain a high level of security awareness. The protection of sensitive data demands regular training of all staff members involved with credit card payment.

- NPRFC will constantly review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day to day company practice.
- NPRFC will distribute this security policy document to all registered staff members to read. It is required that all employees confirm that they understand the content of this security policy document by signing an acknowledgement form (see Appendix A).
- All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS).

Credit Card (PCI) Security Incident Response Plan

- NPRFC PCI Security Incident Response Team (PCI Response Team) is responsible for any security incident plan as follows.

1. All staff members must report an incident to the Information Security Officer (preferably) or to another member of the PCI Response Team.
2. That member of the team receiving the report will advise the PCI Response Team of the incident.
3. The PCI Response Team will investigate the incident and assist all external agencies in limiting the exposure of cardholder data and in mitigating the risks associated with the incident.
4. The PCI Response Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (credit card associations, credit card processors, etc.) as necessary.
5. The PCI Response Team will determine if policies and processes need to be updated to avoid a similar incident in the future, and whether additional safeguards are required in the environment where the incident occurred, or for the institution.

North Petherton RFC PCI Security Incident Response Team

Communications Director	Nick Rees
Compliance Officer	Sharon Sweet
Information Security Officer	Sharon Sweet

Collections & Card Supplier Services	Tracey Evans
Risk Officer	Wayne Carter

Incident Response Notification

First Level Escalation Members

Information Security Officer
Executive Project Director for Credit Collections and Merchant Services Legal Counsel
Risk Manager

Second Level Escalation members

North Petherton RFC President
Executive Committee
Internal Audit

External Contacts (as needed)

Merchant Provider
Card Brands
Internet Service Provider (if applicable)
Insurance Provider
External Response Team as applicable. Law Enforcement Agencies as applicable inn local jurisdiction

In response to a systems compromise, the PCI Response Team and designees will:

1. Ensure compromised system/s is isolated on/from the network.
2. Contact external agencies and entities as appropriate.
3. Make forensic and any diary analysis available to appropriate law enforcement or card industry security personnel, as required.
4. Assist law enforcement and card industry security personnel in investigative processes, including in prosecutions.

The credit card companies have individually specific requirements that the Response Team must address in reporting suspected or confirmed breaches of cardholder data. See below for these requirements.

Incident Response notifications to various card schemes

1. In the event of a suspected security breach, alert the Information Security Officer immediately.
2. The Information Security Officer will carry out an initial investigation of the suspected security breach.
3. Upon confirmation that a security breach has occurred, the Information Security Officer will alert the Response Team and begin informing all relevant parties that may be affected by the compromise.

VISA Steps

If the data security compromise involves credit card account numbers, the following procedure will be implemented:

- A shut- down any systems or processes involved in the breach to limit the extent, and prevent further exposure.
- An alert to all affected parties and authorities such as the Merchant Bank (the Clubs bank), Visa Fraud Control, and the police.
- NPRFC will provide details of all compromised or potentially compromised card numbers to Visa Fraud Control within 24 hrs.
- For more Information visit: http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_if_compromised.html

Visa Incident Report Template

This report must be obtained from and returned to VISA within 14 days after an initial report of such an incident to VISA. The following report content and standards must be followed when completing the incident report. Incident report must be securely distributed to VISA and the Clubs bank. Visa will classify the report as "VISA Secret"*.

I. Executive Summary
   a. Include overview of the incident
   b. Include RISK Level(High, Medium, Low)
   c. Determine if compromise has been contained
II. Background
III. Initial Analysis
IV. Investigative Procedures
   a. Include forensic tools used during investigation
V. Findings
   a. Number of accounts at risk, identify those stores and compromised
   b. Type of account information at risk
   c. Identify ALL systems analysed. Include the following:
      - Domain Name System (DNS) names
      - Internet Protocol (IP) addresses
      - Operating System (OS) version
      - Function of system(s)
   d. Identify ALL compromised systems. Include the following:
      - DNS names
      - IP addresses
      - OS version
      - Function of System(s)
   e. Timeframe of compromise
   f. Any data exported by intruder
   g. Establish how and source of compromise
   h. If applicable, review VisaNet endpoint security and determine risk
VI. Compromised Entity Action
VII. Recommendations
VIII. Contact(s) at entity and security assessor performing investigation

MasterCard Steps:

I. Within 24 hours of an account compromise event, notify the MasterCard Compromised Account Team via phone at 1-636-722-4100.
II. Provide a detailed written statement of fact about the account compromise (including the contributing circumstances) via secured e-mail to compromised_account_team@mastercard.com.
III. Provide the MasterCard Merchant Fraud Control Department with a complete list of all known compromised account numbers.
IV. Within 72 hours of knowledge of a suspected account compromise, engage the services of a data security firm acceptable to MasterCard to assess the vulnerability of the compromised data and related systems (such as a detailed forensics evaluation).
V. Provide weekly written status reports to MasterCard, addressing open questions and issues until the audit is complete to the satisfaction of MasterCard.
VI. Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.
VII. Provide finding of all audits and investigations to the MasterCard Merchant Fraud Control department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of MasterCard.

Once MasterCard obtains the details of the account data compromise and the list of compromised account numbers, MasterCard will:

1. Identify the issuers of the accounts that were suspected to have been compromised and group all known accounts under the respective parent member IDs.

2. Distribute the account number data to its respective issuers.

Discover Card Steps

I. Within 24 hours of an account compromise event, notify Discover Fraud Prevention at (800) 347-3102
II. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances
III. Prepare a list of all known compromised account numbers
IV. Obtain additional specific requirements from Discover Card

American Express Steps

I. Within 24 hours of an account compromise event, notify American Express Merchant Services at (800) 528-5200 in the U.S.
II. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances
III. Prepare a list of all known compromised account numbers Obtain additional specific requirements from American Express

Transfer of Sensitive Information Policy

- All third-party companies providing critical services to North Petherton RFC must provide an agreed Service Level Agreement.
- All third-party companies which have access to Card Holder information must

1. Adhere to the PCI DSS security requirements.
2. Acknowledge their responsibility for securing the Card Holder data.
3. Acknowledge that the Card Holder data must only be used for assisting the completion of a transaction, supporting a loyalty program, providing a fraud control service or for uses specifically required by law.
4. Have appropriate provisions for business continuity in the event of a major disruption, disaster or failure.
5. Provide full cooperation and access to conduct a thorough security review after a security intrusion by a Payment Card industry representative, or a Payment Card industry approved third party.

Review

This policy will be reviewed every two years Wayne Carter Nov 2023

Appendix A
Agreement to Comply With Information Security Policy

Employee Name:

Department: Clubhouse Bar

I agree to take all reasonable precautions to assure that Club internal information, or information that has been entrusted to the Club by third parties such as customers, will not be disclosed to unauthorised persons. At the end of my employment or contract with the Club, I agree to return all information to which I may 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 Information Security Officer who is the designated information owner.
I have access to a copy of the Information Security Policy and other policies as published on the Clubs web page. I have read and understand these policies, and I understand how it impacts upon my job. As a condition of continued employment, I agree to abide by the policies and other requirements found in the above policies. I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties.
I also agree to promptly report all violations or suspected violations of information security policies to the Information Security Officer.

_____
Employee Signature

_____
Date

Appendix B – List of Devices

Asset/Device Name	Description	Owner/Approved User	Location
VeriFone Vx670	Hand held device		Behind the Bar
VeriFone Vx670	Hand held device		Behind the Bar
VeriFone Vx670	Hand held device		Behind the Bar
VeriFone Vx670	Hand held device		Behind the Bar
VeriFone Vx670	Hand held device		Behind the Bar
VeriFone Vx670	Hand held device		Behind the Bar
VeriFone Vx670	Hand held device		Behind the Bar
VeriFone Vx670	Hand held device		Behind the Bar
VeriFone Vx670	Hand held device		Behind the Bar
VeriFone Vx670	Hand held device		Behind the Bar

Appendix C - List of Service Providers

Name of Service Provider	Contact Details	Services Provided	PCI DSS Compliant	PCI DSS Validation Date
NONE				