St. Paul's Boxing Academy CIO

CARDHOLDER INFORMATION

SECURITY POLICY

St Paul's Boxing Academy CIO

CARDHOLDER INFORMATION SECURITY POLICY

1. Introduction

St Paul's Boxing Academy CIO is committed to respecting and securing the privacy of all our members, coaches, Trustees and visitors. The introduction of pay as you go subscriptions means that St Paul's holds sensitive cardholder information.

This policy sets out the safeguards in place to protect cardholder privacy, to ensure regulatory compliance and to guard the integrity of the charity.

2. Objectives of the Information Security Policy

a) To ensure the privacy of members' cardholder data is secured through rigorous safeguards.

b) To ensure the charity's compliance with Payment Card Industry Data Security Standard (PCIDSS) regulations which is to be validated annually.

3. Statement of Intent

Volunteers, coaches and Trustees handling sensitive cardholder data will:

a) ensure cardholder information is treated sensitively and in accordance with this policy and with St Paul's Privacy Policy;

b) not disclose personnel information unless authorised by the chair of the Management Working Group

c) protect sensitive cardholder information;

d) keep passwords and accounts secure;

e) always leave desks clear of sensitive cardholder data and lock computer screens when unattended;

f) report information security incidents without delay to the chair of the Management Working Group.

We all have a responsibility for ensuring St Paul's Boxing Academy CIO's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies you should seek advice and guidance from a member of the Management Working Group.

4. Operation

a) Protection of stored data

- All sensitive cardholder data must be securely protected against unauthorised use at all times. Any sensitive card data that is no longer required 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.
- PAN'S which are not protected as stated above should not be sent to the outside network via end user messaging technologies like chats, ICQ messenger etc.

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.

b) Access to cardholder data

Access to cardholder data will be controlled and authorised by the Management Working Group.

- Any display of the card holder data should be restricted at a minimum of the first 6 and the last 4 digits.
- Access to sensitive cardholder information is restricted to those that have a legitimate need to view such information.

c) Physical security

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

- Authorised users of the card reader are responsible for the security of their passwords and accounts.
- Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals. Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drive, etc.
- All Point of Sale (POS) and Personal Identification Number (PIN) entry devices should be protected and secured so they cannot be tampered with or altered.
- Strict control will be maintained over the external or internal distribution of any media

containing card holder data and has to be approved by Trustees.

- Strict control is maintained over the storage and accessibility of media.

d) 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.
- On-line data will be permanently deleted when no longer required.
- All hard copies of cardholder data will be manually destroyed when no longer required for valid and justified business reasons.
- All cardholder information awaiting destruction will be held in the safe in containers clearly marked “To Be Shredded” - access to these containers is restricted.

5. Breaches

Any failure to uphold the standards and procedures described in this document will result in disciplinary action including termination of membership. Claims of ignorance, good intentions or using poor judgment will not be accepted as reasons for non-compliance.

Related Policies

St Paul’s Privacy Policy

St Paul’s CCTV Policy

Reviewed: November 2022

Next Review: November 2023

Agreement to comply with St Paul's Boxing Academy CIO
Data Security Policy and Cardholder Information Security Policy

Name (printed) _____

Position _____

I agree to take all reasonable precautions to ensure that internal information, or information that has been entrusted to St Paul's Boxing Academy CIO by third parties such as members, will not be disclosed to any unauthorised persons.

If I leave St Paul's Boxing Academy CIO, 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 Trustees.

I have read and understand St Paul's Data Security Policy and Cardholder Information Security Policy.

- ✓ I agree to abide by both these 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 agree to promptly report all violations or suspected violations of these information security policies to the Club Welfare Officer.

Signature _____ **Date:** _____