Scarborough
College

PCI DSS POLICY

Information Security Awareness Program

All employees authorised to accept payment cards (debit and credit cards) securely process, store and dispose of payment card data (paper and electronic media) in order to adhere to the Payment Card Industry Data Security Standards (PCI DSS).

In order to protect cardholder data and ensure PCI DSS compliance at Scarborough College, the following procedures are followed:

- Authorised employees comply with the PCI DSS
- All e-commerce transactions use Flywire's secure online site. Manual transactions use Lloyds Bank PLC secure terminal
- Payment card data is not transmitted or stored in any other system, server, personal computer or e-mail account. Under no circumstance is credit card information obtained, or transmitted, by e-mail
- Physical (paper) cardholder data is locked in a secure filing cupboard with access limited to only authorised employees. These printed materials may include, but are not limited to, paper receipts
- All media used for credit cards is destroyed once the transaction is completed. All hardcopy (paper) is crosscut shred prior to disposal

PCI DSS Compliance Guidelines

- It is against Scarborough College Policy to store credit card numbers on any computer, server, database or spreadsheet
- Restrict access to card data by business need to know
- Paper documents containing cardholder data must be locked securely
- Restrict physical access to cardholder data
- Email is not an approved way to transmit credit card numbers
- Paper receipts must be destroyed so that account information is unreadable and cannot be reconstructed
- Any new systems/software that process payment cards are required to be approved by the Business Manager prior to being purchased
- Maintain a firewall and router configuration to protect cardholder data
- Use and regularly update anti-virus software
- Do not use vendor-supplied defaults for systems passwords and other security parameters
- Computer systems using "Virtual Terminal" must be connected to the proprietary sub-domain with no network access
- Report all suspected or known security breaches to the Business Manager

Payment Card Industry Data Security Standards (PCI DSS) for Accepting Credit Cards

PCI compliance is required of all merchants and service providers that store, process, or transmit cardholder data. The requirements apply to all payment channels, including retail (in person), mail/telephone order, and e-commerce.

Scarborough College is required by the payment card associations to be compliant with the Payment Card Industry (PCI) Data Security Standards, and is committed to providing a secure environment for our customers to protect against both loss and fraud. Scarborough College must comply with Payment Card Industry (PCI) requirements for securely processing, storing, transmitting and disposing of cardholder data.

The PCI DSS is a result of collaboration among the major payment card companies to create common industry security requirements, aiming to protect against both cardholder data exposure and compromise.

The PCI DSS offers a single approach to safeguarding sensitive data for all payment card companies. Other card companies have also endorsed the PCI DSS within their respective programs.

The PCI DSS consists of twelve basic requirements;

PCI Security Standard	
Build and Maintain a Secure Network	■ Install and maintain a firewall configuration to protect data ■ Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	■ Protect stored data ■ Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Management Program	■ Use and regularly update anti-virus software ■ Develop and maintain secure systems and applications
Implement Strong Access Control Measures	■ Restrict access to data by business need-to know ■ Assign a unique ID to each person with computer access ■ Restrict physical access to cardholder data
Regularly Monitor and Test Networks	■ Track and monitor all access to network resources and cardholder data ■ Regularly test security systems and processes
Maintain an Information Security Policy	■ Maintain a policy that addresses information Security

Policy Prepared by:

Alison Higgins (Miss)
Business Manager

Person Responsible for Updates	Date Last Reviewed	Next review due
Alison Higgins	October 2022	October 2023