SELBY TOWN COUNCIL – INFORMATION SECURITY POLICY
Compliance Date - 9 August 2017

1. Introduction

This Policy Document encompasses all aspects of security surrounding confidential company information and must be distributed to all company employees. All company employees must read this document in its entirety and sign the form confirming they have read and understand this policy fully. This document will be reviewed and updated by Management on an annual basis or when relevant to include newly developed security standards into the policy and distribute it all employees and contracts as applicable.

2. Information Security Policy

Selby Town Council 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.

Selby Town Council commits to respecting the privacy of all its customers and to protecting any data about customers from 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.

Employees handling Sensitive cardholder data should ensure:

- Handle Company and cardholder information in a manner that fits with their sensitivity;
- Do not disclose personnel information unless authorised;
- Protect sensitive cardholder information;
- Always leave desks clear of sensitive cardholder data

We each have a responsibility for ensuring the Town Council's systems and data are protected from unauthorised access and improper use. If you are unclear seek advice and guidance from the Town Clerk.

3. Acceptable Use Policy

The Town Council's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Selby Town Council's established culture of openness, trust and integrity. Management is committed to protecting the employees, partners and Selby Town Council from illegal or damaging actions by individuals, either knowingly or unknowingly. Selby Town Council will maintain an approved list of devices and personnel with access to such devices as detailed in Appendix B.

- Employees should take all necessary steps to prevent unauthorized access to confidential data which includes card holder data.
- Keep passwords secure and do not share card holder data.
- Authorized users are responsible for the security of their passwords and card holder data.

4. Disciplinary Action

Violation of the standards, policies and procedures presented in this document by an employee will result in disciplinary action, from warnings or reprimands up to and including termination of employment. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for non compliance.

5. Protect Stored Data

- All sensitive cardholder data stored and handled by Selby Town Council and its employees must be securely protected against unauthorised use at all times.
- Any sensitive card data that is no longer required by Selby Town Council for business reasons must be discarded in a secure and irrecoverable manner.

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.

6. Access to the sensitive cardholder data

All Access to sensitive cardholder 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 of the first 6 and the last 4 digits of the cardholder data.
- Access rights to privileged user ID's should be restricted to least privileges necessary to perform job responsibilities
- Privileges should be assigned to individuals based on job classification and function (Role based access control)
- Selby Town Council will ensure that a there is an established process including proper due diligence is in place before engaging with a Service provider.
- Selby Town Council will have a process in place to monitor the PCI DSS compliance status of the Service provider.

7. 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.

- Employees should take all necessary steps to prevent unauthorized access to confidential data which includes card holder data.
- 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
- 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 appropriate personnel.

- A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- Visitors must always be escorted by a trusted employee when in areas that hold sensitive cardholder information.
- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- All computer that store sensitive cardholder data must have a password protected screensaver enabled to prevent unauthorised use.

8. Disposal of Stored Data

- All hard copies of cardholder data must be manually destroyed as 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.
- Selby Town Council will have procedures for the destruction of hardcopy (paper) materials. These will require that all hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed.
- All cardholder information awaiting destruction must be held in lockable storage containers clearly marked “To Be Shredded” - access to these containers must be restricted.

9. Roles and Responsibilities

- The Town Clerk is responsible for overseeing all aspects of information security, including but not limited to:
- Creating and distributing security policies and procedures.
- Monitoring and analysing security alerts and distributing information to appropriate members of staff
- Monitor and control all access to data.
- Maintain a list of service providers.
- Ensure there is a process for engaging service providers including proper due diligence prior to engagement.
- Maintain a program to verify service providers’ PCI-DSS compliant status, with supporting documentation.
- Ensuring that employees acknowledge in writing at least annually that they have read and understand Selby Town Council’s information security policy.
- Written contracts require adherence to PCI-DSS by the service provider.
- Written contracts include acknowledgement or responsibility for the security of cardholder data by the service provider.

Key staff involved in Card Payment transactions are:

- Town Clerk
- Resource Manager
- Senior Administration Officer
- Administration Officers
- Arts Officer

Appendix A – Agreement to Comply Form – Agreement to Comply With Information Security Policies

_____
Employee Name (printed)

_____
Department

I agree to take all reasonable precautions to assure that company internal information, or information that has been entrusted to Selby Town Council by third parties such as customers, will not be disclosed to unauthorised persons. At the end of my employment or contract with Selby Town Council, 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 internal manager who is the designated information owner.

I have access to a copy of the Information Security Policy, I have read and understand the policy, and I understand how it impacts my job. As a condition of continued employment, I agree to abide by the policy and other requirements found in Selby Town Council security policy. 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 designated security officer.

_____
Employee Signature

Appendix B

Asset/Device Name	Description	Owner/Approved User	Location
Terminal	World Pay Terminal	Selby Town Council	Town Hall Office

List of Service Providers

Name of Service Provider	Contact Details	Services Provided	PCI DSS Compliant	PCI DSS Validation Date
World Pay	03308080663	Card Payment	Yes	9.8.17

Date of Approval	25.9.17
Latest date of next Review	8.8.18
Cross Reference Documents	