SELBY TOWN COUNCIL (the Council)

INFORMATION TECHNOLOGY SECURITY POLICY

This Policy encompasses all aspects of security surrounding confidential information and must be distributed to all relevant employees and councillors. All relevant 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 at a time determined by Council or when relevant to include newly developed security standards into the Policy and distribute it to all relevant employees and councillors.

The information the Council holds and the Information Technology (IT) systems and networks that support it are important business assets. Many potential threats to these exist, such as fraud, vandalism, virus infection, theft, loss, abuse of copyright, misuse of software and accidental damage.

Scope

This Policy is mandatory and there are no exceptions to it. It applies to all relevant employees of the Council, councillors, contractors, agents and partners, who have authorised access to the Council's IT systems. This Policy applies throughout the lifecycle of information held by the Council on all types of media, from its receipt or creation, storage and use, to disposal.

Policy Statement

The Council understands the importance of information security and privacy. It is increasingly dependent on IT systems and so the potential impact of any breach is also increasing. The Council must safeguard its information systems and ensure compliance with this Policy, to provide protection from the consequences of information loss, damage, misuse or prosecution.

The General Data Protection Regulation 2018 (GDPR) places a duty on the Council to demonstrate accountability and to have in place the organisational and technical measures to protect the personal data it holds and processes. The Council is committed to providing the levels of information security required to protect this data

and this Policy helps to set out how the Council aims to achieve the necessary standards. We also aim to fulfil the business needs of the Council and to allow staff to work in a flexible way, whilst maintaining the security levels required.

Contents

1. Controls

The Council has information security measures in place to help mitigate risk, known as controls. These controls are divided into three categories: administrative, technical and physical.

Administrative Controls
A written Information Technology Security Policy (this document) is available to all. Employees are required to read and sign this Policy.

All authorised users of the Council's IT equipment and systems have responsibilities to protect information assets and comply with information security procedures. However, the Town Clerk has overall accountability and responsibility for understanding and addressing information risk, including within their own service areas and for assigning ownership for information assets to others.

Technical Controls
Technical controls are addressed within this Policy and comprise the IT network and its software protection programmes.

Physical Controls
Physical controls are addressed within this Policy and comprise the human behaviours and disciplines put in place by our IT users to provide protection**.**

2. Network Security

The Council's network is backed up daily onto an external hard drive. The Council uses 2 hard drives and these are alternated. The back-up hard drives are stored in the fireproof cabinet. A third backup is taken weekly onto an external hard drive and store off site at the 1811 Building. The portable backup drives are encrypted.

Back up zip files of RBS data are sent monthly to be stored externally by Rialtas Business Software.
The Council uses Microsoft 365 which is a cloud-based system for emails and file storage.
A monthly server support package is in place which includes scheduled back-ups and disaster recovery.
The biggest risk to the Council's IT system is incoming viruses from the World Wide Web. Mitigation of this risk is covered in this Policy.

Security of passwords is essential, and each user is responsible for the security of their passwords.

All PCs owned by the Council will be equipped with suitable antivirus software to protect the Council from computer virus infections and other harmful programs:

- If you suspect the equipment, you are using may be infected, switch off and disconnect from the network. When this is done, report to the Town Clerk as soon as possible.
- Email itself is rarely harmful; it is primarily documents or programs attached to an email that can contain viruses. If you do not recognise the sender, or have any doubts at all about an email, do not open it; it is better to delete it. Never open attachments or click on links within an email unless you are certain you know where the email has come from
- Websites are another source of viruses. The Council's anti-virus software will automatically detect any viruses before anything is downloaded. If you see a warning message, leave the website and contact the Town Clerk.

Be vigilant when browsing the internet and accessing web-based personal email systems using council equipment. If a computer virus is transmitted to another organisation, the Council could be held liable. So always take care, do not open anything suspicious and, if in doubt contact the Town Clerk.

3. Secure Configuration

All computers/laptops should allow updates when prompted to ensure that they are properly patched with the latest appropriate updates, to reduce system vulnerability and enhance and repair application functionality.

4. User Training and Awareness

All authorised users must receive appropriate training, including information technology security requirements. It is the responsibility of the Town Clerk to ensure all staff undertake the training provided. All new employees are to be made aware and sign this Policy as part of their induction.
The Council's IT equipment and systems may only be used for the conduct of personal purposes in line with the Council Communications Policy. Under no circumstances can Council IT systems be used for private commercial activity. Failure to comply may result in disciplinary action for staff, or councillors being reported to the Monitoring Officer.

5. Malware Prevention

Do not copy licensed software, install or use unlicensed software. Software is protected by copyright.

Do not download material such as fonts, drivers, shareware or freeware without proper authorisation from the Town Clerk.
Do not copy or download material or publish it on the Council's website unless you have permission to do so. Much of the material on the internet is protected copyright. The Council retains copyright over material produced.

If the presence of malware is suspected contact the Council's IT support.

6. Home Working

Staff and councillors who use portable corporate devices, such as laptops, tablets and mobile phones, must be particularly vigilant since these devices are more likely to be lost, damaged or stolen.

Authorised working from remote locations such as home or conference is permitted. Care must be taken when using Council IT infrastructure away from the office to ensure that portable devices are:

- Not left unattended in a public place
- Not left in view in unattended vehicles
- Not be taken abroad unless permission is approved by the Town Clerk.

7. Incident Management

All security incidents must be reported immediately to the Town Clerk. All authorised users have a responsibility to promptly report any suspected or observed incident.

Incidents that result from deliberate or negligent disregard of any security policy requirements may result in disciplinary action being taken. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for non-compliance.

All incidents will be recorded and reviewed, so they can be effectively managed.

8. Record of Users

The Town Clerk will maintain a record of approved devices and personnel with access to such devices as detailed in Appendix D.

9. Roles and Responsibilities

The Town Clerk is responsible for overseeing all aspects of information security, including but not limited to:

a. Creating and distributing security policies and procedures
b. Monitoring and analysing security alerts and distributing information to appropriate members of staff
c. Monitor and control all access to data
d. Maintain a list of service providers
e. Ensure there is a process for engaging service providers including proper due diligence prior to engagement
f. Maintain a program to verify service providers' PCI-DSS (Payment Card Industry Data Security Standard) compliant status, with supporting documentation
g. Ensuring that all relevant Councillors and employees acknowledge in writing, when the policy is issued or updated, that they have read and understand the Council's Information Technology Security Policy

h. Written contracts require adherence to PCI-DSS by the service provider
i. Written contracts include acknowledgment or responsibility for the security of cardholder data by the service provider

Payment Data Security – Acceptable Use Policy

10. Introduction

The 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.
The Council commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end the Council 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:

- They 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 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.

The Council's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to the Council's established culture of openness, trust and integrity. The Council is committed to protecting the employees, partners and the Council from illegal or damaging actions by individuals, either knowingly or unknowingly.

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

11. Protect Stored Data

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

It is strictly prohibited to store:

- The contents of the payment card magnetic strip (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

12. 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 IDs 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)
- The Council will ensure that a there is an established process including proper due diligence is in place before engaging with a Service provider.
- The Council will have a process in place to monitor the PCI DSS (Payment Card Industry Data Security Standard) compliance status of the Service provider.

13. 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 unauthorised 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 customer, visitor, 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.

14. Disposal of stored data

- 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.
- The Council have procedures for the destruction of hardcopy (paper) materials – all hardcopy materials are shredded 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.

15. Key staff

Key staff involved in Card Payment transactions are:

- Town Clerk
- Deputy Town Clerk
- Arts Officer
- Facilities Manager
- Market/Events Manager
- Administration Officers

Date of Approval	Jan 2024
Latest date of next Review	July 2028
Cross Reference Documents	Privacy Policy/Notice Communications Policy

Appendix A – Agreement to Comply Form – Agreement to Comply with Information Security Policies (Town Council Staff only)

_____
Employee Name (printed)

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 Town Clerk who is the designated information owner.

I have access to a copy of the Information Technology 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 Information Technology 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 Town Clerk.

_____
Employee Signature

Appendix B – Agreement to Comply Form – Agreement to Comply with Information Security Policies (Councillors only)

_____
Councillors Name (printed)

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 term 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 Town Clerk who is the designated information owner.

I have access to a copy of the Information Technology Security Policy, I have read and understand the policy, and I understand how it impacts my role as a Councillor.

I also agree to promptly report all violations or suspected violations of information security policies to the Town Clerk.

_____
Councillor Signature

Appendix C - Agreement to Comply Form – Agreement to Comply with Information Security Policies (Contractors only)

_____

Name (Printed)

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 contract/work 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 Town Clerk who is the designated information owner.

I have access to a copy of the Information Technology Security Policy, I have read and understand the policy, and I understand how it impacts my role as a contractor.

I also agree to promptly report all violations or suspected violations of information security policies to the Town Clerk.

_____
Signature

Appendix D

Asset/Device Name	Description	Owner/Approved User	Location
Terminal	World Pay Terminal	Selby Town Council	Town Hall Office
Terminal	Sum Up	Selby Town	1811

		Council	
Terminal	Sum Up	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	Jan 2025
Sum Up	020 3510 0160	Card Payment		