

# SILEBY PARISH COUNCIL

## CYBER SECURITY POLICY

### Introduction

The risk of data theft, scams, and security breaches can have a detrimental impact on the Council's systems, technology infrastructure and reputation. As a result, Sileby Parish Council has created this policy to help outline the security measures put in place to ensure information remains secure and protected.

### Purpose

The purpose of this policy is to:

1. Protect Sileby Parish Council's data and infrastructure.
2. Outline the protocols and guidelines that govern cyber security measures
3. Define the rules for council and personal use
4. List the council's disciplinary process for policy violations.

### Scope

This policy applies to all of Sileby Parish Council's councillors, officers, remote workers, permanent and part-time employees, contractors, volunteers, suppliers and/or any individuals with access to the council's electronic systems, information, software, and/or hardware.

### Confidential Data

Sileby Parish Council defines "confidential data" as:

- i Unreleased and classified financial information.
- ii Customer and supplier information.
- iii Employees' passwords and personal information.
- iv Council contracts and legal records.

### Device Security

#### 1. Council Use

To ensure the security of all council-issued devices and information, Sileby Parish Council employees are required to:

- 1.1 Keep all council-issued devices, including tablets, computers, and mobile devices, password-protected (minimum of 8 characters).
- 1.2 Secure all devices before leaving their desk.
- 1.3 Obtain authorisation from the clerk before removing devices from council premises.
- 1.4 Refrain from sharing private passwords with colleagues, personal acquaintances and councillors.
- 1.5 Regularly update devices with the latest security software.

2/.....

## **2. Personal Use**

Sileby Parish Council recognises that employees and Councillors may be required to use personal devices e.g. mobile phones, to access council systems. In these cases, employees are responsible for ensuring the devices used are protected.

To ensure council systems are protected, all employees are required to:

- 2.1 Keep all devices password-protected or secure
- 2.2 Install antivirus software or appropriate operating system protection
- 2.3 Regularly upgrade antivirus software where available
- 2.4 Lock all devices if left unattended.
- 2.5 Always use secure and private networks when accessing Council systems

## **3. Email Security**

Protecting email systems is a high priority as emails can lead to data theft, scams, and carry malicious software like worms and bugs. Therefore, Sileby Parish Council requires all employees to:

1. Verify the legitimacy of each email, including the email address and sender name.
2. Avoid opening suspicious emails, attachments, and clicking on links.
3. Look for any significant grammatical errors.
4. Avoid clickbait titles and links.
5. Contact the Clerk regarding any suspicious emails.

## **4. Transferring Data**

Sileby Parish Council recognises the security risks of transferring confidential data internally and/or externally. To minimise the chances of data theft, we instruct all employees to:

1. Refrain from transferring classified information to employees and outside parties.
2. Only transfer confidential data over Sileby Parish Council networks or secure private networks
3. Obtain the necessary authorisation from the Clerk, if appropriate
4. Verify the recipient of the information and ensure they have the appropriate security measures in place.
5. Immediately alert the Parish Council of any breaches, malicious software, and/or scams.