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, Frampton Cotterell Parish Council has created this policy to help outline the security measures put in place to ensure information remains secure and protected.

The National Cyber Security Strategy describes 'cyber security' as: 'the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures.'

With councils making more local public services available digitally, getting more of their workforce online, and planning greater collaboration and integration work with partner organisations, reviewing and reinforcing current cyber security arrangements is a key priority for the Council. A cyber incident can be very disruptive, leading to the loss of data, as well as disruption to the running of council services.

Those with criminal or hostile intent will continue to try to breach our security to steal the data we hold and/or damage our systems. Therefore, the Council need to continuously review, refresh, and reinforce its approach to cyber security.

This threat cannot be eliminated completely, but the risk can be greatly reduced to a level that allows us to benefit from the huge opportunities that digital technology brings to public services.

Purpose

The purpose of this policy is to:

1. Protect Frampton Cotterell 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 company's disciplinary process for policy violations.

Scope

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

Confidential Data

Frampton Cotterell Parish Council defines "confidential data" as:

1. Unreleased and classified financial information.

2. Customer and supplier information.

3. Employees' passwords and personal information.

4. Council contracts and legal records.

Device Security

1. Council Use

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

1.1 Keep all Council issued devices, including tablets and Chromebooks, computers, and mobile devices, password-protected with a secure password

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 anyone including colleagues, personal acquaintances, and councillors.

1.5 Regularly update devices with the latest security software.

Passwords

All devices shall be protected by:

• EITHER a password containing:

- At least 8 characters, including at least 1 each of the following:
  - ▪ Uppercase letter
  - ▪ Lowercase letter
  - ▪ Digit
  - ▪ Special character, examples !”£$%^&*()_-+={[}]:@~;’#<>?/

• OR a local PIN that is not easily guessable.

• OR fingerprint, retina, or facial recognition.

Security Software

Firewalls must be used where available. For Windows 10 devices Defender must be used, and for all devices with Windows operating systems earlier than Windows 10, effective antivirus software must be installed and used.

Personal Use

Frampton Cotterell Parish Council recognises that employees may be required to use personal devices e.g. mobile phones, to access company systems. In these cases, employees must report this information to management for record-keeping purposes. Mobile phones should not be used unless there is a good reason to do so. Authorisation should first be obtained from the Clerk.

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

2.1 Keep all devices password-protected.

2.2 Ensure all personal devices used to access Council-related systems are password protected.

2.3 Install antivirus software as recommended by the I.T. contractor.

2.4 Regularly upgrade antivirus software.

2.5 Lock all devices if left unattended.

2.6 Ensure all devices are always protected.

2.7 Always use secure and private networks.

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, Frampton Cotterell Parish Council requires all employees and councillors 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. Council to policy is to always air on the side of precaution and immediately delete any suspicious emails. Suspicious emails should be shift deleted to ensure they are removed from devices.

3. Look for any significant grammatical errors.

4. Avoid clickbait titles and links.

5. Contact the Clerk regarding any suspicious emails.

Transferring Data

Frampton Cotterell 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 and councillors to:

1. Refrain from transferring classified information to employees and outside parties.

2. Only transfer confidential data over Frampton Cotterell Parish Council networks.

3. Obtain the necessary authorisation from the Clerk.

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.

Data held on Office 365

When a councillor ceases to be member of the Council, their Office 365 account will be immediately suspended and then deleted when no further access to the data is required by the Council, usually within 30 days.

When an officer ceases to be employed by the Council, access to their Office 365 account will be removed. Access to the account will usually be given to their replacement or another officer.

Removing Council data from devices

When a councillor ceases to be a member, or an officer ceases to be employed, they must remove all Council data from their personal devices. Similarly, when a councillor or officer no longer uses a personal device for Council business, all Council data on that device must be removed. Council devices are to be handed to the Clerk upon leaving and the passwords given. The Clerk will ascertain whether any Council data needs to be removed from such device. It is usual to hand devices to the incoming Officer or Member and they may require the Council data on the device.

Data removal must be by either:

• physical destruction of the data storage

• or wiping with a suitable utility (ask the Clerk for recommendation of a suitable utility at the time the device is changed).

In addition, Council data must be permanently deleted on any associated cloud storage other than the council's Office 365 system. If required by the Council or the Clerk, the councillor or officer must sign a statement confirming that all data has been removed.

HR documents

All current HR documents must be stored in a secure Office 365 folder to which only the Clerk has access. Any HR documents that must be maintained on paper must be stored securely by the Clerk in a locked cabinet.

Some HR data is held by external HR contractors. Council will ensure that the contractor submits confirmation that the data is held securely.

Physical media

Any physical media concerning Council business such as paper documents printed by, or in the possession of councillors or officers, other than public documents must be:

• When not stored in a dwelling that is locked when not in use e.g. a councillor's or officer's home, kept in a locked container such as a metal filing cabinet.

• Shredded as soon as they have been used for the purpose for which they were produced. All Officers and Members should refer to the Data Retention Policy for further details.

Insurance

The Council will hold appropriate cyber security insurance at all times.