

Burnham Market Parish Council IT Usage and Security Policy for Staff and Council Members

Introduction

The purpose of this policy is to ensure that all staff and council members use Parish Council IT equipment responsibly and safely. This includes using it for Council-related tasks, protecting against viruses and cyber threats, complying with security measures, and managing sensitive information appropriately.

This policy aims to protect both the Parish Council's IT assets and the security of the data and systems in use.

Appropriate Use of IT Equipment

- **Council Equipment:** All IT equipment, including computers, tablets, smartphones, and peripherals (such as printers and scanners), provided by the Parish Council is for official Council business only.
- **Usage Restrictions:** Personal use of Council IT equipment should be kept to an absolute minimum. Council devices should not be used for personal emails, social media, or accessing non-work-related websites.
- **Respect for Equipment:** All users should take reasonable care to avoid damaging equipment. Devices should not be dropped, exposed to water, or subject to physical stress (e.g., rough handling or dropping).

Internet and Network Access

- **Safe Browsing:** Internet use on Council devices should be limited to accessing websites relevant to Council work. Users should avoid visiting sites that are not related to Council activities or may contain inappropriate or harmful content.
- **Protecting Against Cyber Threats:** To mitigate the risk of hacking or viruses, users must adhere to the following practices:
 - **Use Only Authorized Software:** Only software and applications approved by the Parish Council should be installed on Council devices.
 - **Virus Protection:** Ensure that all internet activity, including emails and downloads, is done through devices with up-to-date antivirus software. This software must be configured to run automatic scans regularly.
 - **Safe Internet Connections:** When accessing the internet remotely (e.g., from home), ensure that the device is connected to a secure network. Avoid using public Wi-Fi networks for accessing sensitive information.
 - **Multi-Factor Authentication (MFA):** All Council members and staff must use MFA where available for accessing any Council systems, email, and shared files to prevent unauthorized access.

Security Measures

- **Password Protection:** Strong passwords must be used for all Council accounts, systems, and devices. Passwords should be at least 8 characters long and include a combination of upper and lowercase letters, numbers, and special characters.
- **Locking Devices:** When leaving an IT device unattended, it must be locked or logged off. Devices should be password-protected, and screens should be locked when not in use to prevent unauthorized access.
- **Data Encryption:** All sensitive Council data stored on devices must be encrypted to protect information from unauthorized access, particularly if the device is lost or stolen.
- **Compliance with Policies:** Users must comply with any other security measures or guidelines issued by the Parish Council, including software updates and firewalls, to ensure ongoing protection against risks.
- **Downloads and local storage:** Data and sensitive information must not be downloaded and stored locally on Tablets and Laptops with the exception of an encrypted external hard drive
- **Data back ups:** All data is stored online through one drive (or secure equivalent) . All data will be monthly backed up to an encrypted external hard drive stored securely by the clerk.

Handling Lost or Stolen Equipment

In the event that a Council device is lost, stolen, or left unattended where it might be accessed by unauthorized individuals, users must follow these steps immediately:

1. **Contact the Parish Clerk:**
 1. Notify the Parish Clerk immediately to report the loss or theft.
 2. The Clerk will block access to Council email accounts through NALC
 3. The clerk will block access to all Sharepoint files either by password protecting the whole drive, or moving to an offline location) and request from IT supplier that the user be logged out and passwords reset.
2. **Remote Wiping**
 1. No documents are downloaded to Tablets so remote wiping is unnecessary; access passwords will be reset to prevent access to emails and shared drives.
 2. No documents are held on the Clerk's Laptop all are online and will be remote wiped by the clerk accessing from an alternative laptop.
3. **Access Revocation:** The Clerk will revoke access to email accounts, shared files, and any other cloud-based services used for Council work to prevent unauthorized access.

4. **Report to Authorities:** In cases of theft, report the incident to the local authorities for further action.
5. **Replacement Equipment:** If the device is not recoverable, the Clerk will arrange for a replacement device following the Council's asset management procedures.

General Responsibilities

- **Compliance:** All staff and council members are responsible for adhering to this policy and ensuring the safe use of Council IT equipment.
- **Reporting Issues:** Any security breaches, suspicious activity, or potential risks should be reported immediately to the Parish Clerk.
- **Training:** All staff and council members will be required to undergo training on cybersecurity and the responsible use of IT equipment, including the use of MFA, virus protection, and secure internet practices.

Consequences of Misuse

Failure to follow the guidelines outlined in this policy may result in disciplinary action, including the loss of access to IT equipment and systems, depending on the severity of the breach.