

Burnham Market Parish Council

IT Usage and Security Policy for Staff and Council Members

Adopted: 09/12/24

Review: Biannually

Last reviewed: [insert date]

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.

Internet and Network Access

- **Safe Browsing:** Internet use should be limited to Council-related activities. Users should avoid accessing inappropriate or non-work-related sites.
- **Protection Against Cyber Threats:**
 - Only approved software may be installed.
 - Devices must have up-to-date antivirus protection with automatic scanning enabled.
 - Public Wi-Fi should be avoided when accessing Council systems unless appropriately secured (e.g. via VPN or equivalent protection).
 - Multi-Factor Authentication (MFA) must be used where available for Council systems, email, and shared files.

Security Measures

- **Password Protection:** Strong, unique passwords or passphrases must be used for all accounts and devices.
- **Locking Devices:** Devices must be locked or logged off when unattended.
- **Data Protection:** Sensitive Council data should be protected using appropriate security measures, including encryption where systems allow and where appropriate to the level of sensitivity.
- **Downloads and Storage:** Sensitive information should not be stored locally on devices unless necessary for Council business and protected appropriately.
- **Backups:** Council data is stored in secure cloud systems (e.g. OneDrive or equivalent). Regular backups are undertaken to ensure data integrity and recovery capability.

Handling Lost or Stolen Equipment

In the event of loss or theft of a Council device, the following steps must be taken immediately:

1. Report to the Parish Clerk immediately.
2. The Clerk will arrange for access to Council systems (email, shared drives, cloud services) to be revoked or reset.
3. Where applicable, passwords will be reset and access disabled to prevent unauthorised use.
4. If theft is suspected, the incident will be reported to the police.
5. Replacement equipment will be arranged in accordance with Council asset procedures.

Data Breach Reporting (UK GDPR Compliance)

Where a personal data breach occurs or is suspected, it must be reported immediately to the Parish Clerk.

The Clerk will assess the breach and determine whether it is reportable to the Information Commissioner's Office (ICO).

Where required under **UK GDPR Article 33**, reportable breaches will be notified to the ICO **within 72 hours of the Council becoming aware of the breach**, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals.

Where the risk is high, affected individuals will also be notified in accordance with **UK GDPR Article 34**.

General Responsibilities

- All users are responsible for complying with this policy.
- Any security incidents or suspicious activity must be reported immediately to the Parish Clerk.
- Staff and councillors may be required to undertake periodic training on IT security and safe use of systems.

Consequences of Misuse

Failure to comply with this policy may result in restricted access to Council IT systems and/or disciplinary action depending on the severity of the breach.