ST MABYN PARISH COUNCIL

INFORMATION TECHNOLOGY POLICY

Introduction

St Mabyn Parish Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications. This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by council members, Clerk, volunteers, and contractors.

Purpose of the IT Policy

The purpose of an IT policy is to establish clear parameters for how councillors, staff, and other authorised users use council-provided technology or equipment in the course of their duties. This policy will:

- Set expectations for appropriate use of equipment and systems;
- Raise awareness of risks associated with IT use;
- Safeguard the council's data and digital assets;
- Clarify what constitutes acceptable and unacceptable use;
- Outline the consequences of policy breaches.

Scope of this policy

This policy applies to all individuals who use St Mabyn Parish Council's IT resources, including computers, software, devices, data, and email accounts.

1. Monitoring of IT Use

As an IT provider, the council has the right to monitor the use of its IT equipment, resources and email, provided there is a legitimate reason for doing so and councillors, employees and other authorised users are informed that such monitoring may take place. Any monitoring must be proportionate and comply with relevant data protection and privacy laws.

2. Acceptable use of IT resources and email

St Mabyn Parish Council's IT resources and email accounts are to be used for official council-related activities and tasks. Limited personal use is permitted, provided it does not interfere with work responsibilities or violate any part of this policy. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

3. Device and software usage

Where possible, authorised devices, software, and applications will be provided by St Mabyn Parish Council for work-related tasks. Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

4. Data management and security

All sensitive and confidential St Mabyn Parish Council data should be stored and transmitted securely using approved methods. Regular data backups should be performed to prevent data loss, and secure data destruction methods should be used when necessary.

5. Network and internet usage

St Mabyn Parish Council's network and internet connections should be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited.

6. Email communication

Email accounts provided by St Mabyn Parish Council are for official communication only. Emails should be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless it is encrypted. Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

7. Password and account security

St Mabyn Parish Council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others. Regular password changes are encouraged to enhance security.

8. Mobile devices and remote work

Mobile devices provided by St Mabyn Parish Council should be secured with passcodes and/or biometric authentication. When working remotely, users should follow the same security practices as if they were in the office.

9. Retention and archiving

Emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an organised inbox.

10. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the Clerk for investigation and resolution. Report any email-related security incidents or breaches to the Clerk immediately.

11. Training and awareness

St Mabyn Parish Council will provide regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will receive regular training on email security and best practices.

12. Policy review

This policy will be reviewed annually to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

13. IT-related enquiries or assistance

Clerk and councillors are responsible for the safety and security of St Mabyn Parish Council's IT and email systems. By adhering to this IT and Email Policy, St Mabyn Parish Council aims to create a secure and efficient IT environment that supports its mission and goals.

This Policy was adopted by St Mabyn Parish Council on 3rd February 2026