St Austell Bay Parish Council

Information Technology (IT) Policy

Introduction

St Austell Bay Parish Council recognizes 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, employees, volunteers, and contractors.

1) Purpose

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. It ensures the council's digital operations are transparent, secure and compliant. 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.

2) 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.

3) Scope

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

4) Acceptable Use of IT Resources and Email

St Austell Bay 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.

5. Device and Software Usage

Where possible, authorized devices, software, and applications will be provided by St Austell Bay Parish Council for work related tasks. All software installations must be approved and logged by the Clerk or designated IT contractor.

6 Data Management and Security

All sensitive and confidential St Austell Bay 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.

7 Network and Internet Usage

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

8 Email Communication

The use of personal email accounts for council business is strictly prohibited. All council correspondence must be conducted through official council-provided email addresses. Emails should be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless encrypted. Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links

9 Password and Account Security

St Austell Bay 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. Multi-factor authentication should be used where possible.

10 Mobile Devices and Remote Work

Mobile devices provided by St Austell Bay 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.

11 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 organized inbox.

12 Data Breach Process and Protocols

The Parish Council is committed to responding promptly and effectively to any data breaches to minimize risk and comply with UK GDPR and DPA requirements.
Any councillor, employee or contractor who becomes aware of a data breach must report it immediately to the Clerk.

Definition of a Data Breach : A data breach is a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
Examples include:

- Loss or theft of devices containing personal data
- Unauthorised access to council email accounts or files
- Sending personal data to the wrong recipient
- Malware or ransomware attacks compromising council systems

13 Training and Awareness

St Austell Bay 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.

14 Policy Review

This policy will be reviewed annually to ensure its relevance and effectiveness or following a significant incident or legislative change.

15 IT-Related enquiries or Assistance

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

This Policy was adopted by St Austell Bay Parish Council on 19th March 2026