Feock Parish Council

IT Policy

Adopted February 2026

Feock Parish Council IT Policy

Contents

This IT Policy was adopted by the council at its meeting held on Monday 9th February 2026.

1. Purpose
The purpose of this IT Policy is to establish guidelines for the responsible and secure use of information technology (IT) resources within the Parish Council. This policy ensures that all IT systems, devices, and networks are used efficiently, securely, and in compliance with relevant legislation, including data protection laws and good governance practices.

2. Scope
This policy applies to all members, staff, volunteers, contractors, and any other individuals who have access to the Parish Council's IT resources, including computers, email, internet, and other digital platforms.

3. IT Resources
The following are considered IT resources of the Parish Council:

- **Computers & Laptops**: Used for council-related activities.
- **Email Systems**: Official council email accounts for communication.
- **Internet Access**: For council-related research and communication.
- **Network Infrastructure**: Servers, routers, and network equipment.
- **Software & Applications**: Licensed software tools used for council work.

4. Acceptable Use
- **Authorised Use**: IT resources should be used for council business only. Personal use is allowed but should be kept to a minimum.
- **Security**: Users are responsible for securing their devices and accounts. Passwords must be kept confidential. An envelope with passwords for Parish Council systems for all members of staff is locked in the safe in the event these are needed by Councillors in an emergency. Focus Technology Europe, Unit 3, Woodmine Business Park, Semmens Wy, Redruth TR15 1FU, tel: 01209 613660 are able to override passwords to access Council laptops.
- **Data Protection**: Personal and council-related data must be managed in accordance with data protection laws, including GDPR. Unauthorized sharing of data is prohibited.

5. Internal Controls and Accountability
To ensure the integrity and security of IT resources, the following internal controls are in place:

- **Monitoring and Logging**: IT systems will be regularly monitored for compliance with this policy. Access logs will be reviewed periodically by the Council Chair or Clerk/RFO.
- **Audit Trails**: Systems processing sensitive or financial data will maintain audit trails, which will be reviewed for unauthorized access or anomalies.
- **Access Control**: Access to sensitive data is restricted to authorized personnel based on their roles. Regular reviews of access permissions will be conducted.

6. Fraud Prevention and Detection
The Parish Council is committed to preventing, detecting, and responding to fraud involving IT systems:

- **Secure Transactions**: Financial and confidential transactions will be processed using secure systems with multi-factor authentication and encryption.
- **Reporting Suspicious Activity**: Any suspicious activity, such as unauthorized access or fraudulent actions, should be reported immediately to the Council Chair or Clerk/RFO.
- **Data Loss Prevention (DLP)**: Measures will be in place to prevent the unauthorized loss, leak, or misuse of sensitive data.

7. Internet and Email Use

- **Appropriate Content**: Council IT resources must not be used to access or transmit illegal, offensive, or inappropriate material.
- **Email Etiquette**: Emails should be professional, respectful, and related to council business. Personal use of email should be minimal.
- **Email Security**: Emails from untrusted sources should be handled with caution. Attachments should only be opened from known and trusted senders.

8. Software and Licensing

- **Licensing**: All software used must be properly licensed. The use of pirated software is strictly prohibited.
- **Updates**: Regular updates to software and systems will be managed to ensure the latest security patches and functionality.

9. Data Management

- **Data Storage**: All official data will be securely stored in cloud services or council-managed servers. Data will be encrypted where appropriate.
- **Data Sharing**: Sensitive data will be shared only with authorised individuals, using secure methods.
- **Data Retention and Disposal**: Data will only be retained for as long as necessary and in accordance with the Council's GDPR policy and securely disposed of once no longer required.

10. IT Risk Management

The Parish Council will regularly assess IT-related risks to ensure systems remain secure and resilient:

- **Cybersecurity Measures**: Regular updates and security scans will be performed to protect against cyber threats.
- **Backup Procedures**: All critical data will be regularly backed up to ensure business continuity in case of system failure or data loss. Backups will be tested periodically.
- **Staff Training**: All council staff and members will receive training on basic cybersecurity practices, including safe use of passwords and identifying phishing attempts.

11. Social Media and Public Communication

- **Council Accounts**: Only authorized individuals may post on official council social media accounts.
- **Personal Use**: Personal social media accounts should not be used for council-related business. All public-facing communications must align with council values.
- **Representation**: When using personal social media accounts, council members must clearly state that the opinions expressed are personal, not those of the council.

12. Mobile Devices

- **Council Devices**: Mobile devices provided by the council must be used primarily for work-related purposes and must be secured with strong passwords. Any sensitive data on these devices should be backed up.
- **Personal Devices**: Personal devices may be used for council-related work with approval, but they must comply with the council's security protocols and data protection standards.

13. Compliance with Data Protection Laws

The Parish Council is committed to complying with all relevant data protection laws, including GDPR:

- **Data Processing**: All personal data will be processed in a lawful, fair, and transparent manner.
- **Access to Personal Data**: Personal data will be accessible only to those who need it for their duties, and access will be logged.
- **Data Subject Rights**: The Parish Council will facilitate requests for access, correction, or deletion of personal data as required by law.
- **Data Retention**: Personal data will be kept only for as long as necessary for council purposes and will be securely destroyed when no longer required.

14. Review and Audit

This policy will be reviewed annually to ensure it remains effective and compliant with changing regulations and best practices. The council will also conduct regular audits of its IT systems, including assessments of IT security and data protection practices.

15. Breach of Policy

Any breach of this policy, including unauthorised access, misuse of IT resources, or failure to adhere to security practices, will result in disciplinary action. Breaches must be reported immediately to the Council Chair or Clerk/RFO.

Signatures

By signing below, I acknowledge that I have read, understood, and agree to comply with Feock Parish Council's IT Policy.

Councillor/Staff Member Name: _____

Signature: _____

Date: _____