FEATHERSTONE PARISH COUCIL

27th May 2026, Min Ref: 25/26.06

IT & Email Policy

1. Introduction

Featherstone Parish Council recognizes the importance of using information technology (IT) and email safely, responsibly, and effectively. IT systems support the Council's daily work, decision-making, and communication with residents and partners.

This policy sets out clear, simple rules for how IT equipment and email should be used by councillors, employees, volunteers, and contractors.

2. Scope

This policy applies to everyone who uses Featherstone Parish Coucil IT resources, including computers, mobile devices, networks, software, data, and email accounts.

3. Acceptable Use of IT and Email

Council IT systems and email accounts are primarily for official Council business. Limited personal use is permitted provided it does not interfere with Council duties or breach this policy. Users must act responsibly, legally, and ethically at all times.

4. Devices and Software

The Council will provide approved devices and software where possible. Only authorised software may be installed on Council devices. Personal or unauthorised software is not permitted.

Council devices should be kept updated with appropriate security patches, antivirus protection, and software updates where applicable.

5. Data Management and Security

Confidential and sensitive information must be stored and shared securely. Regular backups should be carried out, and data must be securely deleted when no longer required.

6. Network and Internet Use

Internet access must be used responsibly and mainly for Council business. Downloading or sharing copyrighted material without permission is prohibited.

7. Email Use and Communication

Councillors and staff should use Council-issued email accounts wherever possible for Council business. Emails should be professional and respectful. Sensitive information must not be sent unless appropriately secured. Users should remain cautious of phishing emails, suspicious attachments, and fraudulent communications.

8. Password and Account Security

Users must keep passwords secure, strong, unique, and confidential. Multi-factor authentication should be enabled where available. Passwords must not be shared unless required for business continuity arrangements approved by the Council.

9. Mobile Devices and Remote Working

Council-issued mobile devices must be secured with passcodes or biometric protection. The same security standards apply when working remotely.

10. Email Monitoring

The Council reserves the right to monitor the use of Council IT systems and email accounts where necessary and proportionate, in accordance with the Data Protection Act 2018 and UK GDPR.

11. Email Retention and Archiving

Emails must be retained and archived in line with legal requirements. Unnecessary emails should be deleted appropriately.

12. Reporting Security Incidents

All suspected IT or email security incidents, including data breaches, phishing attempts, or loss of devices, must be reported immediately to the Clerk or Chair of the Council.

13. Data Protection and Records

The Council will process and retain personal data in accordance with its Data Protection Policy, Privacy Notices, UK GDPR, and the Data Protection Act 2018. Records should only be retained for as long as necessary and disposed of securely.

14. Business Continuity

The Council must ensure that critical records, passwords, and account access information can be accessed by authorised persons in the event of staff absence, incapacity, or departure.

15. Training and Awareness

The Council will provide IT and email security training as required. Councillors and staff are expected to participate.

16. Compliance and Consequences

Failure to comply with this policy may result in suspension of IT access or further action.

17. Policy Review

This policy will be reviewed annually and updated as required.

18. Contacts

For IT support or advice, users should contact the designated Council IT contact.

19. Clerk Handover

In the event of the Clerk leaving the Council, all passwords, IT equipment, storage devices, records, and Council-owned digital assets must be transferred to the Chair or another nominated representative of the Council.

Date: M Meadale. vice chairman. 27 May 2026

Signature: _____

Role: _____