Puxton Parish Council

Referred to herein as the parish council

IT and Email Policy

This policy was created and approved by the council its meeting of March 5th 2026 at minute 029/26 iv It will be reviewed annually and updated as necessary to ensure its relevance and effectiveness.

1. Introduction
The 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, employees, volunteers, and contractors.

2. Scope
This policy applies to all individuals who use the parish council's IT resources, including computers, networks, software, devices, data, and email accounts.

3. Acceptable use of IT resources and email
The parish council 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.

4. Device and software usage
Where the parish council provides authorised devices, software and applications will be provided by the parish council for work-related tasks. Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

Where the Clerk to the Council works from their own computer parish council work must be backed up to the Cloud or to some other appropriate external device. Both the original and backup data must be encrypted. Strict security and decency protocols must be observed for non-parish council data held and/or worked on on the computer and a full antivirus and other available security applications must be operating.

5. Data management and security
All sensitive and confidential 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.

6. Network and internet usage
The parish council's network (if there is one) and internet connections should be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited.

7. Email communication
Email accounts provided by the 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.

8. Password and account security
The 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.

9. Mobile devices and remote Work
Mobile devices are not routinely provided by the parish council. Should they be, they must be secured with passcodes and/or biometric authentication. When working remotely, users should follow the same security practices as if they were in the parish council office (if there is one) or their home office.

10. Email monitoring
The parish council reserves the right to monitor email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR.

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 organised inbox.

12. Reporting security incidents
All suspected security breaches or incidents should be reported immediately to the Chair of the parish council.

13 Training and awareness
The parish council will support the Clerk and Councillors in course attendance as needed to provide training and resources relating to IT security best practices, privacy concerns, and technology updates.

14. Compliance and consequences
Breach of this IT and Email Policy by the Clerk or a Councillor may result in an investigation by the parish council, resulting in consequences as deemed appropriate.

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

End of document