

IT Policy Approved Oct 2026 Review annually

1. Introduction

East Dean and Friston 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 councillors, employees, volunteers, and contractors.

Emerging Technologies and AI The parish council acknowledges the rapid evolution of digital tools, including Artificial Intelligence (AI), as part of emerging technologies that can enhance efficiency and service delivery. While these technologies offer significant benefits, their use must remain secure, transparent, and compliant with data protection and ethical standards. This policy includes guidance on responsible AI usage to ensure that it is employed to support achievement of the council's objectives, without compromising accountability or public trust.

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. 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

Since devices are not provided by the council, councillors may use their own devices in accordance with this policy.

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 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. Users must be cautious with attachments and links to avoid phishing and malware and should 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

Any mobile devices provided by The 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 office based.

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. Users should 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 designated IT point of contact for investigation and resolution. Users should report any email-related security incidents or breaches to the Parish Clerk immediately.

13. Training and awareness

All employees and councillors will receive training when required on IT and email security and best practices, privacy concerns and technology updates.

14. Artificial Intelligence (AI) Usage

The Parish Council recognises the potential benefits of Artificial Intelligence (AI) in improving efficiency and supporting service delivery. To ensure responsible and secure use the following apply.

Approved Use: AI tools may be used for administrative support, data analysis, and customer service enhancements.

Transparency & Accountability: all AI-assisted activities must maintain human oversight. Users should be aware that AI content carries risks of inaccuracy and bias; with output reviewed to include checks for accuracy. Material generated by AI should include a statement, stating its significant use in its production.

Data Protection: AI systems must comply with UK GDPR and council data handling policies. Sensitive or confidential data must not be entered into public AI platforms unless anonymised.

Security: only council-approved AI tools may be used. Public or unverified AI services are prohibited for official work.

Ethical Standards: AI must not introduce bias or discrimination.

Training: staff and councillors using AI tools should complete training on responsible AI use and data protection.

Incident Reporting: any suspected misuse or malfunction of AI systems must be reported immediately to the Clerk.

15. Compliance and consequences

Breach of this IT and Email Policy may result in the suspension of IT privileges and further consequences as deemed appropriate.

16. 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.

17. Contacts

For IT-related enquiries or assistance, users can contact the clerk.

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