ST PINNOCK PARISH COUNCIL

IT & Digital Governance Policy

Based on Government Digital Service Template. June 2025 (NALC)

1. Introduction

St.Pinnock 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 principles, guidelines and responsibilities for the appropriate use of IT resources and email by council members, employees, volunteers, and contractors in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. The policy aims to safeguard both the confidentiality and integrity of sensitive information, ensure the council's compliance with legal obligations, and provide clear expectations for acceptable use of IT resources.

2. Scope

This policy applies to all employees, councillors, volunteers, and contractors who have access to the Parish Council's IT systems, networks, and data. It includes the use of all council-owned devices (e.g., laptops, desktop computers, mobile phones), networks, and services such as email, file storage, and website platforms.

3. Acceptable use of IT resources and email

St.Pinnock Parish Council's IT resources and gov.uk 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 possible, authorised devices, software, and applications may be provided to the Clerk or Responsible Financial Officer by St.Pinnock Parish Council for work-related tasks.
Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

5. Data management and security

All data must be accessed, used and protected in compliance with the data protection principles in the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Sensitive personal data (e.g. residents' addresses, contact details and financial information) should only be accessed by those who require it for their Council work. Data should be stored securely on council-approved systems with appropriate access controls in place. Councillors and employees are required to take reasonable steps to ensure that data is securely disposed of when no longer needed. Secure data destruction methods should be used when necessary.
All devices connected to the council's network must have up-to-date antivirus software installed and running. Employees must lock their devices when not in use, especially when working in public places.
Regular data backups should be performed **[…specify how often…]** to prevent data loss. Any device or service storing backups of council data must be secure, approved, risk-assessed, and compliant with the Data Protection Act 2018 and UK GDPR regulations.

6. Network and internet usage
St.Pinnock 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
Gov.uk Email accounts provided by St.Pinnock Parish Council to the Clerk and Councillors are for official communication only. Emails should be professional and respectful in tone.
The use of personal email accounts is discouraged, to ensure records are appropriately retained by the council and are subject to valid Freedom of Information (FOI) requests.
Users are required to be cautious with attachments and links to avoid phishing and malware, to verify the source before opening any attachments or clicking on links.
All Councillors and employees are responsible for the safety and security of St.Pinnock Parish Council's IT and email systems. By adhering to this IT and Digital Governance Policy, St.Pinnock Parish Council aims to create a secure and efficient IT environment.

8. Password and account security
All passwords for council systems should be strong, consisting of at least 12 characters, with a mix of uppercase, lowercase, numbers, and special characters. Passwords should not be shared, and multi-factor authentication (MFA) should be enabled wherever possible.
Staff and councillors should be trained to recognise phishing emails. Any suspicious email, especially those asking for personal or financial information, should be reported immediately.

9. Mobile devices and remote work
Mobile devices provided by St.Pinnock Parish Council should be secured with passcodes and/or biometric authentication.
All software installed on council-owned devices must be legally licensed. Employees are prohibited from installing unauthorised software or using pirated software.
When working remotely, employees and councillors must connect to the council's network via a secure connection. All remote devices should meet the council's security standards, including having up-to-date antivirus software and encrypted communication.

10. Email monitoring
Monitoring will be conducted in accordance with the Data Protection Act 2018, GDPR legislation and The Data (Use and Access) Act 2025. With prior notification to the Chairman of a specific reason, time interval and relevant email account on every occasion, the Clerk may access emails issued by, or received by, Councillors for administrative, security, and legal compliance purposes.
FOI Requests: Emails are also be subject to the Freedom of Information Act 2000.

11. Freedom of Information Act 2000
In the event of a valid request made to St.Pinnock Parish Council under The Freedom of Information Act 2000 by individuals or public bodies with the right to access recorded information held by St.Pinnock Parish Council, the Clerk and Chairman will jointly be given access to all emails issued by, and received by, Councillors and the Clerk within their official gov.uk email accounts relevant to the Freedom of Information request, providing that

information is not subject to Absolute Exemption or Qualified Exemption under the Freedom of Information Act 2000.

12. Retention and archiving
Emails should be retained and archived in accordance with statutory and regulatory requirements. The Clerk and Councillors are required to regularly review accounts and archive or delete unnecessary emails.

13. Reporting security incidents
Any IT-related incident, such as a suspected data breach, cyberattack, or system failure, should be reported immediately to the Clerk. All incidents will be logged and investigated in line with GDPR's breach notification requirements.

14. Training and awareness
St.Pinnock Parish Council will provide training and resources, when necessary, to educate users about IT security best practice, privacy concerns, and technology updates.

15. Compliance and consequences
Breach of this IT and Digital Governance Policy may result in the suspension of IT privileges and further consequences as deemed appropriate.

16. Policy review
This policy will be reviewed **[annually/every 2 years/every 3 years]** 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 should contact the Clerk who may raise the issue with the officially appointed Webmaster if required.