



INFORMATION TECHNOLOGY AND EMAIL POLICY

1. Introduction

Hannington 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 and employees.

2. Scope

This policy applies to all individuals who use Hannington Parish Council's IT resources, including computers, software, devices, data, and email accounts.

3. Acceptable use of IT Resources and Email

Hannington 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 Software Usage

An authorised device, software, and applications (where applicable) will be provided by Hannington Parish Council to the Parish Clerk.

Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

Council Members are expected to use their own IT equipment to access their Council provided email account.

Operating systems and software should be kept up to date on all personal devices. The use of firewalls and antivirus software is recommended for all devices used for council email and document review (free versions are available).

5. Data Management and Security

All sensitive and confidential Hannington Parish Council data should be stored and transmitted securely using approved methods.

Regular data backups should be performed by the Parish Clerk to prevent data loss.

Secure data destruction methods should be used when necessary.

Documents should not be held on personal devices once they are no longer required. This is particularly important in the case of those containing confidential information

6. Email Communication

Email accounts provided by Hannington Parish Council are for official communication only. Emails should be professional and respectful in tone. Confidential or sensitive information must not be shared outside the Parish Council.

The use of personal email accounts for Council business is not allowed.

Hannington Parish Council users should be cautious with attachments and links to avoid phishing and malware. Users should verify the source before opening any attachments or clicking on links.

7. Password and Account Security

Hannington 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.

8. Email Monitoring

Hannington 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.

9. 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.

10. Reporting Security Incidents

All suspected security breaches or incidents should be reported immediately to the Parish Clerk for investigation and resolution. Report any email-related security incidents or breaches to the Parish Clerk immediately.

11. Responsibilities

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

12. Policy Review

This policy will be reviewed annually by the Parish Clerk to ensure its relevance and effectiveness. If required, the Parish Clerk will bring any recommendations or suggested changes before the Council for consideration.

Date of Policy Adoption	10 July 2025
Date of Policy Review	7 July 2026
Agenda Item	39/26
Policy Version number	V2
Date of Next Review	July 2027