Yarnfield and Cold Meece Parish Council

IT and Email Policy (March 2026)

Document title	IT and Email Policy	
Author	Parish Clerk	
Status	Approved	
	Date	Resolution
Approved on	9 March, 2026	26-76
Next review date	March, 2028	

Purpose

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

Contacts

For IT-related enquiries or assistance, users can contact the Clerk in the first instance.

Introduction

1.1 Yarnfield and Cold Meece Parish Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications.

1.2 This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by council members, employees, volunteers, and contractors.

Scope

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

Acceptable use of IT resources and email

1.4 The Parish Council's IT resources and email accounts are to be used only for official council activities and tasks.

Device and software usage

1.5 Where appropriate, the Parish Council will provide devices, software, and applications for work-related tasks of the Parish Clerk.

1.6 Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited.

Bring Your Own Device

1.7 The use of any personal device to access council information is permitted provided strict security measures are in place to protect the device. This includes ensuring the device is not used by anyone else to gain access to council information.

1.8 If you are using your own device, you must make sure you are:

- using strong passwords for all your accounts (preferably using a password manager)
- downloading the latest operating system security updates
- using anti-virus software

Data management and security

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

1.10 Regular data backups should be performed to prevent data loss, and secure data destruction methods should be used when necessary.

1.11 Data back up of all should be done using Microsoft OneDrive.

Network and internet usage

1.12 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.

Email communication

1.13 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.

1.14 Care should be taken when receiving emails that contain either attachments and/or links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

Password and account security

1.15 The Parish Council users are responsible for maintaining the security of their accounts and passwords.

1.16 Email system passwords sorted on Zoho Mail should be strong and not shared with others. Regular password changes are encouraged to enhance security.

Mobile devices and remote work

1.17 Mobile devices provided by Yarnfield and Cold Meece Parish Council should be secured with passcodes and/or biometric authentication.

Email monitoring

1.18 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 General Data Protection Regulations.

Retention and archiving

1.19 Emails should be retained and archived in accordance with legal and regulatory requirements.

Reporting security incidents

1.20 All suspected security breaches or incidents should be reported immediately to the Parsh Clerk to investigate.

Training and awareness

1.21 The Parish Council will provide training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will receive training where a need is identified on email security and best practices.

Compliance and consequences

1.22 Breach of this IT and Email Policy may result in the suspension of IT privileges.

Security Requirements

1.23 All devices must:

- Be secured with a strong password/PIN and auto-lock after inactivity.
- Use encryption where available.
- Be kept updated with operating system and security patches.
- Council data must be accessed only through approved applications (e.g. council email app or secure portal).
- Use of removable media (USBs, SD cards) for council data is prohibited unless encrypted.

Data Protection

1.24 Council data must not be backed up to personal cloud accounts or shared with third-party apps.

1.25 Personal and council data must be kept separate (e.g. using distinct apps).

1.26 Councillors must only use council data for council business.

Loss, Theft, or Leaving Office

1.27 Any loss or theft of a device must be reported immediately to the Clerk.

Monitoring and Compliance

1.28 The Council may require confirmation that devices meet these security standards.

1.29 No monitoring of personal use will be carried out beyond ensuring council data is protected.

Responsibilities

1.30 Councillors remain personally responsible for protecting council data on their device.

Appendix 1