



# Darley and Menwith Parish Council Information Technology Policy

Adopted January 2026

## 1. Introduction

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

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

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 Darley and Menwith Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts.

## 3. Acceptable use of IT resources and email

Darley and Menwith Parish Council IT resources and email accounts are to be used for official council-related activities and tasks. Limited personal use is permitted, provided that 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

Authorised devices, software, and applications will be provided by Darley and Menwith Parish Council where necessary 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 sensitive and confidential Darley and Menwith Parish Council data should be stored and transmitted securely using approved methods. Regular data backups (at least monthly and every time there is an intention to take equipment out of the home office environment) should be performed to prevent data loss, and secure data destruction methods should be used when necessary.

## 6. Network and internet usage

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 Darley and Menwith Parish Council to the Chairman and Clerk 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**

Darley and Menwith 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 provided by Darley and Menwith Parish Council should be secured with passcodes. When working remotely, users should follow the same security practices as if they were in the office.

## **10. Email monitoring**

Darley and Menwith 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 relevant data protection legislation and regulations.

## **11. Retention and archiving**

Emails should be retained and archived in accordance with legal and regulatory requirements. This should include a regular review including deletion of unnecessary emails to maintain an organised inbox.

## **12. Reporting security incidents**

In the event of a suspected security breach or incident, the Darley and Menwith Parish Council Security Incident Policy should be followed.

## **13 Training and awareness**

Darley and Menwith Parish Council will provide regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will receive training on email security and best practices.

## **14. Compliance and consequences**

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

## **15. 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.

## **16. Contacts**

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