

Loders Parish Council

IT and Email Policy

Adopted on: 17th March 2026

1. Introduction

Loders 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, employees, volunteers, and contractors.

2. Scope

This policy applies to all individuals who use IT resources, including computers, networks, software, devices, data, and email accounts and acknowledges that councillors will be using their own personal devices. Everyone must adhere to this policy to maintain digital security.

3. Training and awareness

Loders Parish Council will source regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will engage in regular training on email security and best practices.

4. Acceptable use of IT resources and email

Loders Parish Council IT resources and email accounts are to be used for official council-related activities and tasks. Limited personal use of IT resources or Zoho email 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.

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. Verify the source before opening any attachments or clicking on links.

5. Personal devices

Councillors using their own device must make sure they are:

- Using strong passwords for all their accounts (preferably using a password manager)
- Downloading the latest operating system security updates
- Using anti-virus software, where appropriate

6. Device and software usage

Where possible, IT devices, software, and applications will be provided by Loders Parish Council for work-related tasks.

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

7. Data management and security

All sensitive and confidential Loders Parish Council data should be stored and transmitted securely. Regular data backups should be performed to prevent data loss, and secure data destruction methods should be used when necessary. Email inboxes should be reviewed regularly and unnecessary emails deleted to maintain an organised inbox.

8. Network and internet usage

Loders 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.

9. Password and account security

Loders 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. For business continuity, login details and passwords need to be stored securely so they can be accessed by trusted individuals in an emergency.

10. Mobile devices and remote Work

Mobile devices provided by Loders 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 in the office.

11. Email access

Loders 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. The Clerk may need to access emails so that they can respond to FOI or subject access requests.

12. Reporting security incidents

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

13. Compliance and consequences

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

14. 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.

15. Contacts

For IT-related enquiries or assistance, users can contact the Clerk at Lodders Parish Council.

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