



Oxenhope Village Council

IT & Email Policy

Adopted 11th February 2026

1. Introduction

- 1.1 Oxenhope Village 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 and employees.

2. Scope

- 2.1 This policy applies to all individuals who use the village council's IT resources, including computers, other devices, software and applications, data and email accounts.

3. Acceptable use of IT resources and email

- 3.1 Oxenhope Village Council IT resources and email accounts are to be used for official council-related activities and tasks. Reasonable personal use of IT equipment is permitted, provided it does not conflict with any part of this policy.
- 3.2 All users must adhere to ethical standards, respect copyright and intellectual property rights and avoid accessing inappropriate or offensive content. Downloading and sharing copyrighted material without proper authorisation is prohibited.

4. Device and software usage

- 4.1 Where appropriate, authorised devices, software, and applications will be provided by the council for council related tasks.
- 4.2 Unauthorised installation of software on council provided devices, including personal software, is strictly prohibited due to security concerns.
- 4.3 The council will use Microsoft 365, WhatsApp and Dropbox for communication and file management purposes. Set up and usage advice will be provided as appropriate and the apps required to use these packages maybe installed on personal devices.

5. Data management and security

- 5.1 All sensitive and confidential council data should be stored and transmitted securely using approved methods.

- 5.2 Documents, messages and other files must not be saved outside of the approved applications on personal devices.
- 5.3 Regular data backups will be performed to prevent data loss and secure data destruction methods will be used when necessary.

6. Email communications

- 6.1 An email address using a gov.uk domain will be provided to all councillors and council employees and should be the only address used for official or unofficial council correspondence.
- 6.2 Email accounts provided by the village council are for official communication only.
- 6.3 Emails should be professional and respectful in tone at all times.
- 6.4 Confidential or sensitive information must not be sent to third parties via email.
- 6.5 All users will take account of best practice usage advice and guidance and will exercise caution before opening attachments and clicking on links, to avoid phishing and malware.

7. Password and account security

- 7.1 Village council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others.
- 7.2 All devices provided by the council should be secured with passcodes and/or biometric authentication.
- 7.3 Where users use their own hardware to access council systems or data, they are responsible for ensuring the security of systems and data. Due regard must be had to council policies and procedures on data protection, privacy and document retention.

8. Email monitoring

- 8.1 Oxenhope Village Council reserves the right to monitor email communications to ensure compliance with this policy and relevant legal requirements. Monitoring will be conducted in accordance with the Data Protection Act 2018 and UK GDPR.

9. Retention and archiving

- 9.1 Emails should only be retained in accordance with legal and regulatory requirements. All users will regularly review and delete unnecessary emails to maintain an organised mailbox.
- 9.2 Users must not forward email to their own personal email addresses as a means of archiving and saving mail for future reference (action which would conflict with the council's policies on data protection and privacy).

10. Reporting security incidents

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

11. Training and awareness

- 11.1 From time to time Oxenhope Village Council will provide training and resources to help users with IT security best practices, privacy concerns and technology updates.
- 11.2 All users must keep up to date with best practice and follow security advice and guidance, seeking clarification if required.

12. Compliance

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

13. Policy review

- 13.1 This policy will be reviewed annually to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

14. Contacts

- 14.1 For IT related enquiries or assistance, users can contact the Clerk to the Council.
- 14.2 All staff and councillors are responsible for the safety and security of the village council's IT and email systems. By adhering to this IT and Email Policy, Oxenhope Village Council aims to create a secure and efficient IT environment that supports its mission and goals.