

IT POLICY

1. Introduction

Woodford cum Membris Parish Council [the “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. The Council endeavours to provide digital devices but acknowledges that some Councillors and staff may, on occasion, use their own personal devices. Everyone must adhere to this policy to maintain digital security.

3. Training and awareness

The Council will make available relevant, regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. Engagement is recommended in appropriate training on email security and best practices, including but not limited to:

- the [Parish Council Domain Helper Service’s virtual cybersecurity workshops for councils](#)
- The National Cyber Security Centre [Cyber Security training for small organisations](#) and free [Cyber Action Toolkit](#).

4. Acceptable use of Council provided IT resources and email

When using IT resources for the Council’s purposes, you must adhere to ethical standards, and respect copyright and intellectual property rights.

Where possible, authorised devices, software, and applications will be provided by the Council for its business purposes.

You must not install unauthorised software without checking with the Clerk, and you must not use equipment or email to access or forward inappropriate or offensive content.

5. What you must do if you use your own personal devices

The Council will endeavour to provide individuals with devices for Council business. If you use 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

6. Network and Internet usage

You must be careful about which Wi-Fi networks you join. Public Wi-Fi networks in coffee shops or on trains can be targeted by hackers. Always make sure you are using a trusted internet connection, which is password protected when carrying out official business.

7. Password and account security

You are responsible for maintaining the security of your accounts and passwords. Use the National Cyber Security Centre's [advice for choosing a strong password](#). For business continuity, login details and passwords need to be stored securely so they can be accessed by trusted individuals in an emergency.

8. Email communication

The Council will provide you with an official email account for Council related communication only. If you are currently using a personal email account, you must move to the official email account as soon as practically possible. You must make sure that emails are professional and respectful in tone. You must always check you are sending any confidential or sensitive information to the correct recipients.

Always be cautious when downloading attachments and opening links to avoid phishing and malware. Before opening any attachments or clicking on links, verify the source by looking at the email it has come from carefully. Do not download and open anything if you are unsure who has sent it.

9. Email access

The Council reserves the right to check email communications, in specific circumstances, for compliance with this policy and relevant laws e.g. the Data Protection Act and General Data Protection Regulation. The Clerk may need to access emails in responding to Freedom of Information [FOI] requests &/or Subject Access Requests [SAR].

If you use a personal email account for Council business [which should not be the case as the Council provides everyone entitled with a .gov.uk email account] it is still subject to data protection laws and FOI requests.

10. Data management, data retention and security

All sensitive and confidential data should be stored and transmitted securely. You should regularly backup any important data to prevent loss and archive/retain emails, all according to any requirements set by the Council. A regular review of emails and deletion of unnecessary items is recommended to maintain a clean & clear mail box.

11. Reporting security incidents

All suspected security breaches, including email breaches or incidents should be reported immediately to Cllr. Pete Davies & Gary Smith [the Clerk].

12. Compliance and consequences

Breach of this IT & Email Policy may result in a review of IT uses.

13. 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.

14. Contacts

For IT-related enquiries or assistance, users can contact Cllr. Pete Davies.

All Councillors & staff are responsible for the safety and security of IT and email systems.

This IT Policy is adopted at a meeting of the Council on: 14 April 2026

Council Minute: C70/26

Date for next review: Annual Council Meeting May 2027

gps14iv26