

WEST WRATTING PARISH COUNCIL

IT Policy

1. Introduction

West Wrating Parish Council (WWPC) 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 WWPC's IT resources, including computers, networks, software, devices, data, and email accounts.

3. Acceptable use of IT resources and email

Members of WWPC including the Clerk will be supplied with an account for them to use for parish council matters, including email, data storage, and for access to shared documents. Their password for this account will be shared with the Clerk. They must not use personal email accounts for PC business, and sensitive data must not be saved to personal IT equipment.

West Wrating parish council IT resources and email accounts are to be used for official council-related activities and tasks. Limited personal use 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.

4. Device and software usage

Where possible, authorised devices, software, and applications will be provided by West Wrating parish council 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 West Wrating parish council data should be stored and transmitted securely using approved methods. Regular data backups should be performed to prevent data loss, and secure data destruction methods should be used when necessary.

WEST WRATTING PARISH COUNCIL

6. Network and internet usage

West Wrattling 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.

7. Email communication

Email accounts provided by West Wrattling 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.

Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

When a councillor leaves WWPC they must return control of their email account and data storage to the clerk. When the clerk ends their employment with WWPC they must return control of their account and data storage to the Chair, so that it can be transferred to the new Clerk.

8. Password and account security

WWPC 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 WWPC 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.

10. Email monitoring

WWPC reserves the right to monitor email communications and stored data to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR.

11. Retention and archiving

Emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails.

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 immediately.

WEST WRATTING PARISH COUNCIL

13. Training and awareness

WWPC 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 regular training on email security and best practices. All WWPC councillors and employees will complete [GDPR training](#).

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**.

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

History

This document is based on the template provided by NALC in paragraph 5.122 of the [Practitioner's Guide 2025](#)

April 2025	Original release for review by WWPC
May 2025	Approved at Annual Meeting of the Parish Council and uploaded to website.

Notes:

Paragraph 1.54 of the [Practitioner's Guide 2025](#) says that all smaller authorities (excluding parish meetings) must also have an IT policy.

An [addendum to the 2025 Practitioner's Guide](#) says that Under Section 7 of the DPA 2018, Parish Councils and Parish Meetings are exempt from the requirement to appoint a Data Protection officer (DPO).