Wembdon Parish Council IT Policy

1. Introduction

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

3. Acceptable use of IT resources

Wembdon Parish Council IT resources 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 Wembdon 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 Wembdon 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.

6. Network and internet usage

Wembdon 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 Wembdon 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.

8. Password and account security

Wembdon Parish Council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others. The council follows the National Cyber Security Centre (NCSC) recommendations for creating passwords using three random words (e.g. PurpleCandleRiver). Users should not change their passwords, but regular password changes are encouraged to enhance security and will be provided by the IT administrator at set intervals.

Passwords must not be stored in plain text or written down in insecure locations. Passwords must be stored using a council-approved, encrypted password manager or password protected spreadsheet.

The Clerk has a password protected spreadsheet for all passwords and will provide the password for the spreadsheet to the Chairman, to be used in case of emergency.

Passwords are personal and must not be shared under any circumstances.

Only the assigned user of an account may access or use the associated password. In exceptional cases (e.g., incident response or when an employee or councillor leaves for any reason), access to system credentials may be granted to authorised personnel from the IT provider with appropriate approvals and logging.

9. Mobile devices and Remote Work

Mobile devices provided by Wembdon 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.

10. Email monitoring

Wembdon 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.

11. Retention and archiving

Emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review, delete and purge unnecessary emails to maintain an organised inbox.

When a Councillor leaves the Council, any documents must be destroyed and their email access will be terminated immediately.

12. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the designated IT point of contact for investigation and resolution. Report any email-related security incidents or breaches to the IT administrator immediately.

13 Training and awareness

Wembdon 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 regular 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 every 3 years to ensure its relevance and effectiveness. Interim updates may be made to address emerging technology trends and security measures.

16. Contacts

For IT-related enquiries or assistance, users can contact the IT administrator, currently Councillor Peter Major.

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

Adopted 9th March 2026

To be reviewed as required, at minimum Annually.