OWSLEBURY PARISH COUNCIL

IT and Email Policy

Adopted 12 January 2026

Introduction

Owslebury 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.

Scope

The policy applies to all individuals who use Owslebury Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts.

Acceptable use of IT resources and email accounts

Owslebury Parish Council's IT resources and email accounts are to be used for official council-related activities and tasks. Limited personal use if 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.

Device and software usage

Where possible authorised devices, and applications will be provided by Owslebury Parish Council for work related tasks.

All Council devices will have up-to-date antivirus software installed and this must not be switched off for any reason without authorisation of the Parish Clerk.

All software installed on Council devices must be fully licensed and no software should be installed without authorisation of the Parish Clerk.

Data Management and Data Security

All sensitive and confidential Owslebury Parish Council data should be stored and transmitted securely using approved methods. All data is stored in the cloud to prevent data loss, and secure data destruction methods should be used when necessary.

When using AI, do not use personal information.

Network and Internet Usage

Owslebury 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.

Email communication

All Councillors and employees will be assigned a Council email address as appropriate. This must be used for all Council business.

Email accounts provided by Owslebury Parish Council are for official communications only. Emails should be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless it is encrypted.

Councillors and employees are reminded that any email sent or received in their capacity as a Councillor or member of staff may have to be disclosed following requests under the Freedom of Information Act. This includes emails on personal devices when acting as a Councillor.

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

Password and account security

All Council computers and systems must be password protected to prevent unauthorised access.

Owslebury 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.

Councillors must ensure that when accessing Councillor emails that passwords are protected and access is restricted solely to the member.

Employees should ensure that unattended devices are password protected.

Mobile devices and remote working

Mobile devices provided by Owslebury 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.

Email monitoring

Owslebury 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.

Retention and Archiving

Emails should be retained and archived in accordance with the council's data retention and protection policies and in accordance with any legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an organised inbox.

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.

Training

Owslebury 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.

Compliance and consequences

Any breaches in this IT and email policy will be investigated and any action arising will follow the council's disciplinary procedures.

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.

Contacts

For any queries with reference to this policy, please contact the Parish Clerk

All members of staff and councillors are responsible for the safety and security of Owslebury Parish Council IT and email systems. By adhering to this IT and email policy Owslebury Parish Council aim to create a secure and efficient IT environment.