Milton Malsor Parish Council

IT Policy

1. Introduction

Milton Malsor 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.
The council is committed to ensuring that all IT systems are used securely and responsibly, and in compliance with relevant legislation including the UK General Data Protection Regulation, the Data Protection Act 2018, and information access requirements under the Freedom of Information Act 2000 and the Environmental Information Regulations 2004.

2. Scope

This policy applies to all individuals who use Milton Malsor Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts. This includes councillors, employees, volunteers, contractors, and any third parties who may access council systems or data.

3. Acceptable use of IT resources and email

Milton Malsor Parish Council IT resources and email accounts are to be used for official council-related activities and tasks. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.
Council IT resources must not be used for personal commercial activity, political campaigning, or any unlawful activity. Users should be aware that emails and electronic records created in the course of council business may be subject to disclosure under the Freedom of Information Act 2000 or Environmental Information Regulations 2004.

4. Device and software usage

Where personal devices are used to access council email or documents, users must ensure the device is protected with a password or biometric security and kept up to date with security updates. Council data should not be permanently stored on personal devices where this can be avoided.

5. Data management and security

All sensitive and confidential Milton Malsor 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.
Personal data must be handled in accordance with the UK General Data Protection Regulation and Data Protection Act 2018. Council documents and records should only be stored within approved council systems or authorised cloud storage services.
Adopted and approved at FCM dated 13.11.25 Item 85(c) (iii) Review Date November 2026.

6. Network and internet usage

Milton Malsor 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.
Users must take reasonable precautions to avoid introducing viruses, malware, or other security risks to council systems.

7. Email communication

Email accounts provided by Milton Malsor 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.
Users must ensure that council email accounts are not used to register unauthorised online services or social media accounts representing the council.

8. Password and account security

Milton Malsor 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.
Passwords should be unique, ideally be at least 12 characters long and contain a combination of words, numbers, or symbols. Passwords must not be shared with others.
Where available, multi-factor authentication (MFA) should be enabled on council systems and email accounts.

9. Mobile devices and remote work

Mobile devices 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. Devices should be locked when unattended to prevent unauthorised access.

10. Email monitoring

Milton Malsor 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.
Monitoring will be conducted in accordance with the UK General Data Protection Regulation and the Data Protection Act 2018.

11. Retention and archiving

Emails should be retained and archived in accordance with legal and regulatory requirements.
Regularly review and delete unnecessary emails to maintain an organised inbox.
Records relating to council business must be retained in accordance with the council's records retention policy. Emails and documents relating to council business may be subject to disclosure under the Freedom of Information Act 2000 or Environmental Information Regulations 2004.

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.
All suspected IT security incidents, including phishing attempts, malware infections, or potential data breaches, must be reported immediately to the Clerk.
Where personal data may have been compromised, the council will assess whether notification to the Information Commissioner's Office is required.

13. Training and awareness

Milton Malsor Parish Council may provide regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates as required.
All employees and councillors may receive regular training on email security and best practices as required.

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.
Serious breaches may be dealt with under the council's disciplinary procedures where applicable.

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, Ann Addison on telephone number: 01604 759186 or email: clerk@miltonmalsorparish.gov.uk.
All staff and councillors are responsible for the safety and security of Milton Malsor Parish Council's IT and email systems. By adhering to this IT and Email Policy, Milton Malsor Parish Council aims to create a secure and efficient IT environment that supports its mission and goals.

Reviewed by Milton Malsor Parish Council: March 2026
Adopted by Milton Malsor Parish Council: April 2026
Next Review Date: March 2028