2025
I.T.
POLICY

MARLOW
TOWN COUNCIL

I.T. Policy

Adopted: October 2025

Review Date: October 2026

1. Introduction

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

3. Acceptable use of IT resources and email

Marlow Town 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 Marlow Town Council for work-related tasks.

Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited .

5. Data management and security

All sensitive and confidential Marlow Town Council data should be stored and transmitted securely using approved methods[1]. Regular data backups should be performed to prevent data loss, and secure data destruction methods should be used when necessary.

Never share your Microsoft credentials to access external services unless they have been approved by a responsible MTC officer and IT services provider and only after an appropriate risk assessment has been undertaken.

Sharing your credentials such as Windows or Office login or password could compromise the security of your device and the council's network.

Linking calendars usually requires granting MS Outlook calendar permissions and this is also bad practice as it is creating a data leakage risk and would mean MTC would be

[1] **Data Management and Security**

Marlow Town Council's sensitive and confidential data is securely managed through Microsoft 365, including Office 365 email and SharePoint document storage. All data is transmitted and stored using industry-standard encryption, both in transit and at rest. Access to data is controlled through role-based permissions and Multi-Factor Authentication (MFA) to prevent unauthorized access.
Regular automated backups are managed within Microsoft 365 to protect against data loss. SharePoint and OneDrive versioning features ensure that previous versions of documents can be recovered when necessary. In addition, email and SharePoint data are retained in line with the council's retention policies and GDPR requirements.
When data is no longer required, it is securely destroyed using Microsoft 365's built-in compliance and data loss prevention tools, ensuring full and permanent deletion. Sensitive information is only shared via encrypted email or secure document links within Microsoft 365, avoiding insecure transmission methods.
These measures ensure that Marlow Town Council complies with best practices for data protection, confidentiality, and security, safeguarding all council-related information.
For data in transit, Microsoft 365 uses TLS (Transport Layer Security) 1.2 or higher, ensuring all data transmitted between client devices and Microsoft servers is encrypted end-to-end. This prevents interception or tampering during transmission.

Email (Exchange Online):

TLS 1.2+ is used for mail flow between clients, servers, and external recipients that support TLS.
Office Message Encryption (OME) is available for encrypting sensitive email content, providing message-level encryption and rights management.
SMTP connections are also secured with STARTTLS.

SharePoint Online and OneDrive:

All browser connections to SharePoint and OneDrive use HTTPS with TLS 1.2+.
File uploads and downloads are encrypted using TLS to prevent data exposure during transfer.
All sensitive Marlow Town Council data sent via Office 365 email or stored/retrieved from SharePoint is protected against eavesdropping and tampering by strong encryption protocols, fully compliant with UK GDPR and ISO 27001 standards.

exposed to breaching GDPR regarding the securing of personal information. It should not therefore be done unless approved by a responsible MTC officer and IT services provider and only after an appropriate risk assessment has been undertaken.

6. Network and internet usage

Marlow Town 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 Marlow Town 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

Marlow Town Council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others. A strong password is considered at least 12 characters in length, comprising of a mix of upper and lower case characters, numbers and symbols. Regular password changes are encouraged to enhance security.

9. Mobile devices and remote work

Mobile devices provided by Marlow Town 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

Marlow Town 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 and delete unnecessary emails to maintain an organised inbox.

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

Marlow Town Council will provide regular training and resources to educate users about IT security best practices, privacy concerns, legal obligations (such as compliance with GDPR) 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 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 Town Clerk.

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