MAULDEN PARISH COUNCIL
Information Technology Policy

(*based on the Smaller Authorities Proper Practices Panel 2025 template*)
TO BE READ AND APPLIED IN CONJUCTION WITH THE BRING YOUR OWN DEVICE POLICY

Adopted: July 27, 2026
Next Review Date: Annually

DEFINITIONS USED WITH THIS POLICY
MPC: Maulden Parish Council

MPC IT hardware covers:
- **Hardware, including network facilities, computers and other electronic devices in the care of MPC.**

MPC IT software covers:
- **MPC email facility.**
- **Software, including commercial software in the care of MPC.**

MPC data covers:
- **MPC physical or electronic information, such as documents, passwords, logon details, accounts and emails, whether received or created by MPC.**

MPC IT resources covers:
- **MPC IT hardware, MPC IT software and MPC data**

MPC IT users covers:
- **MPC employees, MPC Councillors, and MPC volunteers who assist MPC usually because of their relevant experience, using MPC IT resources.**

Personal devices covers:
- **Hardware devices not in the care of MPC, including computers, laptops, tablets and phones.**

Cloud covers:
- **A global network of remote servers that store and process data for devices and computers. Companies such as Microsoft, Apple, Google and others, provide a limited free Cloud service to their users.**

1. INTRODUCTION
Maulden Parish Council (MPC) 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 MPC IT resources by MPC IT users**.**

2. SCOPE
This policy applies to all MPC IT users. MPC provide digital devices for employees, but other MPC IT users will use their own personal devices to access MPC IT resources. All MPC IT users must adhere to this policy to maintain digital security, whether using personal devices or MPC-provided hardware.

3. TRAINING AND AWARENESS
MPC will endeavour to source regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates for MPC IT users. For IT-related enquiries or assistance, contact MPC's Clerk via clerk@maulden-pc.gov.uk

4. ACCEPTABLE USE OF MPC IT FACILITIES
When using MPC IT resources all MPC IT users must adhere to ethical standards, and respect copyright and intellectual property rights. Where possible, authorised hardware and appropriate software will be provided by MPC for work-related tasks.
No software is to be installed or used on MPC IT hardware without prior approval from the Clerk.
MPC IT facilities are not to be used to access or forward inappropriate or offensive content.

5. USE OF PERSONAL DEVICES
MPC will provide employees with devices to use for MPC business, other MPC IT users will need to use their own device to access MPC data and MPC email. Please refer to the Bring Your Own Device Policy for guidance on how this should be managed.

6. NETWORK AND INTERNET USAGE
When accessing MPC accounts or email, MPC IT users should ensure a trusted, password-protected, internet connection is used. Public wi-fi networks such as those widely available in shopping centres, coffee shops, buses and trains etc, should not be used as these are readily targeted by hackers using the same open network.

7. PASSWORD AND ACCOUNT SECURITY

MPC IT users are responsible for ensuring their use of MPC IT facilities does not compromise the security of MPC IT resources or of MPC data. As stated above, the use of a strong password that is not shared and the use of secure networks are strongly recommended.

8. EMAIL COMMUNICATION

Email communication by MPC IT users is only conducted using the official MPC email system.
Where appropriate, MPC will provide a MPC IT user with an MPC email account.
MPC email accounts are only for use for MPC-related communications.
MPC IT users should always:

- Make sure that emails are professional and respectful in tone.
- Check that the intended recipients are correct, particularly if the email contains confidential or sensitive information.
- Take care when opening an email particularly if there are attachment or links. Be aware of phishing *(a scam where attackers deceive the recipient into revealing sensitive information)* attempts or inadvertently installing malware (*malicious software designed to harm or exploit a programmable device or network, such as viruses, worms, adware, or ransomware*). The sender's name as shown on the displayed email can be spoofed *where the sender is masquerading as another person.* Clicking on the sender's name shown in the email usually reveals the sender's actual email address. If there are doubts about the sender, do not open the attachment or click on the link.
- Use the following disclaimer in your email. This can be added automatically to emails by including the following text in the MPC email account setup:

MAULDEN PARISH COUNCIL (MPC) DISCLAIMER: This email and any attachments are confidential to the intended addressee and may contain privileged information. If you are not the intended recipient of this email, please notify the sender immediately and delete the message without copying or using it for any purpose. Any disclosure, copying, distribution or any action taken, or omitted to be taken in reliance on it, may be prohibited and could be unlawful. Data in emails could be infected, intercepted or corrupted; however, the sender accepts no liability for any damage caused by viewing the content of this email. By contacting MPC you agree for your contact details to be held and processed for the purposes of correspondence. You may request access to the information MPC hold on you and request to be removed as a contact at any time. To view MPC's Privacy Policy please see https://maulden-pc.gov.uk/policies-and-procedures/

9. EMAIL ACCESS

MPC reserve the right to check email communications using the MPC facility to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR.
MPC's Clerk may need to access MPC emails so they are able to respond to Freedom Of Information (FOI) or subject-access requests (SAR) in a timely manner.
If, contrary to MPC policy, a personal email account is used for MPC business, this will also be subject to data protections laws and FOI requests.

10. DATA MANAGEMENT, DATA RETENTION AND SECURITY

MPC data should be regularly backed up to prevent data loss and to follow MPC's policy on Retention Of Documents & Records. Where documents are stored within a cloud system, the cloud provider will provide that backup. Where stored on a user's personal device, the user has this responsibility.
Emails received should be regularly deleted and backed up in compliance with MPC's policies on Retention Of Documents & Records, Data Protection and GDPR. It is convenient to create a rule within the email server so all emails received are automatically copied to an All Emails Received folder within the email account. Once dealt with, emails should be deleted or moved to an appropriate storage folder within the email account. Such storage folders, once created, will exist on the email provider's servers, their use makes for an organised system in which saved emails can be readily retrieved.

11. REPORTING SECURITY INCIDENTS

All suspected security breaches, including email breaches or incidents should be reported immediately to MPC's Clerk via clerk@maulden-pc.gov.uk.

12. COMPLIANCE AND CONSEQUENCES

Breach of this Information Technology Policy may result in the suspension of IT privileges.
Any MPC IT user found to have deliberately breached the Data Protection Act 2018 or GDPR regulations may be subject to disciplinary measures or referred to the Monitoring Officer.

13. 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.