MAULDEN PARISH COUNCIL
Bring Your Own Device Policy

THIS POLICY MUST BE TAKEN IN CONJUNCTION WITH MPC'S INFORMATION TECHNOLOGY POLICY

Adopted: July 27, 2026
Next Review Date: Annually

CONTENTS
Part 1: Maulden Parish Council BYOD – Quick Guide for Councillors & Specialist Volunteers
Part 2: Policy
Part 3: Maulden Parish Council Bring Your Own Device (BYOD) Declaration

PART 1: MAULDEN PARISH COUNCIL (MPC) BYOD – QUICK GUIDE FOR MPC COUNCILLORS & VOLUNTEERS

This summary explains what you need to know when using your **personal phone, tablet, or computer** for council work. It is in 2 parts:
Section A: MPC Councillors and Volunteers using personal devices with email app and downloading.
B: MPC Councillors and Volunteers using personal devices with webmail only.

SECTION A:
MPC COUNCILLORS AND VOLUNTEERS USING PERSONAL DEVICES WITH EMAIL APP AND DOWNLOADS

1. YOU CAN USE YOUR OWN DEVICE — BUT FOLLOWING THE RULES NECESSARY TO REDUCE THE RISK OF UNAUTHORISED ACCESS TO MPC DATA STORED ON THE DEVICE.

You may use your personal device for:
- MPC email.
- Reading or drafting MPC documents.
- Online meetings for MPC work.
- Accessing approved cloud systems (eg SharePoint, OneDrive, etc).

You **must not** use your device for any MPC:
- Special category data (health, ethnicity, political opinions).
- Safeguarding information,
- HR matters.
- Large datasets of residents' personal information.

If you receive such data by accident, delete it and notify the Clerk.

2. YOUR DEVICE MUST BE SECURE

You must:
- Use a PIN, password, fingerprint, or facial recognition.
- Keep the device updated.
- On laptops/PCs use the latest operating system security updates.
- Keep encryption enabled.
- Lock your screen when not in use.
- Avoid public Wi-Fi unless using a VPN.

MPC data must be stored in **on secure devices only**.

3. KEEP MPC AND PERSONAL DATA SEPARATE

- Do not store MPC documents that are not in the public domain in personal apps (e.g., WhatsApp, Messenger).
- If a personal device is shared then MPC data that is not in the public domain should be held within apps or a section of the device with restricted access. Depending on the device platform, these restricted areas include user accounts, secure folders, and guest modes. Such restricted areas should be exited prior to the personal device being used by a person other than a MPC Councillor or Volunteer.
- MPC cannot access your personal content. In some instances, MPC may need to access only any MPC data stored on your devices, in order to address a specific GDPR issue or Freedom Of Information request, if this is not available elsewhere.

4. IF YOUR DEVICE IS LOST OR STOLEN

Tell MPC's Clerk **immediately**. MPC may need to you to remotely delete **MPC data** from the device.

5. WHEN YOU LEAVE MPC OR STOP VOLUNTEERING YOU MUST:

- Delete all MPC data that is not in the public domain.
- Return or destroy any downloaded documents that are not in the public domain.
- Confirm deletion if asked.

6. EXPENSES

Using your own device is **voluntary**. MPC are **not required** to reimburse device costs unless agreed in advance.

7. YOU MUST SIGN MPC'S BYOD DECLARATION
Before using your personal device for MPC work, you must sign MPC's **BYOD Declaration Form** confirming you understand your responsibilities.

SECTION B:
MPC COUNCILLORS AND VOLUNTEERS USING PERSONAL DEVICES WITH WEBMAIL ONLY

The Easiest Way to Stay GDPR-Compliant
Many MPC Councillors and Volunteers prefer not to have MPC data stored on their personal devices. MPC supports this by a Webmail-Only Option that keeps MPC data off your personal device entirely. **Where a MPC Councillor or volunteer uses MPC's approved webmail only and does not store MPC data on their personal device, MPC will not require access to that device under any circumstances.** This option provides a simple low-risk, privacy-respecting way to stay GDPR compliant.

1. WHAT WEBMAIL-ONLY MEANS
MPC Councillors and Volunteers simply:
- Use the **MPC-approved** webmail in your browser for MPC email services.
- Do not download MPC attachments
- Do not use email apps (Apple Mail, Outlook, BlueMail, etc) for MPC email services.
- Do not save MPC documents to your device.

Your device becomes just a window into MPC's email system.

2. WHAT THIS MEANS FOR YOUR PRIVACY
If you use webmail only:
- No MPC data is stored on your device
- MPC have no lawful basis to access your personal device

This is the least intrusive way to handle MPC email.

3. WHAT YOU STILL NEED TO DO
Just a few simple things:
- Keep your device locked with access control, such as a PIN, password, fingerprint.
- Keep your browser and operating system updated.
- Don't download attachments unless absolutely necessary.
- Report loss or theft of your device (in case your browser was logged in).

4. WHO THIS OPTION IS IDEAL FOR
- MPC Councillors and Volunteers who only need to read and reply to emails.
- Those who prefer to keep MPC data off their personal device

5. WHO SHOULD NOT USE WEBMAIL-ONLY
- MPC's Clerk or employees.
- MPC Councillors handling HR, safeguarding, or sensitive data.
- Anyone who needs to download or edit MPC documents.

6. MPC ACCESS TO PERSONAL DEVICE
If you use **MPC-approved** webmail only, there is no need for MPC to access your personal device to address a GDPR or Freedom Of Information request. All MPC data received/sent by you will be on MPC's approved webmail system.

7. YOU MUST SIGN MPC'S BYOD DECLARATION
Before using your personal device for MPC work, you must sign MPC's **BYOD Declaration Form** confirming you understand your responsibilities.

PART 2: POLICY

Maulden Parish Council (MPC) BYOD Policy (For Clerk, Councillors, and Specialist Volunteers) Terms
'MPC' refers to Maulden Parish Council.
'Volunteer' refers to a non-Councillor assisting MPC, given their particular knowledge or ability, eg planning advisors, IT support, community project leads who have access to MPC email system.
'Personal device' refers to personal electronic devices, such as phones, tablets, laptops and PCs used to access MPC data.
'Deletion' – often, when data on an electronic device is 'deleted', it can be readily restored. In this policy, 'deletion of data' means permanent, irrevocable erasure of data.
Note: *If an employee uses a personal device for work, the employer has to abide by legal requirements regarding data protection, expense reimbursement and privacy.*
*When a **MPC Councillor or Volunteer** uses a **personal device** for MPC-related matters, MPC still carry **many of the same legal responsibilities** as they would with an employee — especially around **data protection (GDPR)** and **privacy** - but **not** the same obligations around **employment and rights** such as expense reimbursement.*

GDPR applies to the data, not the employment status of the person handling it.

If a MPC Councillor or Volunteer uses a personal device for MPC work:

- MPC must treat them as a **data processor,** that is handling or processing data on behalf of MPC, according to MPC's instructions.
- MPC must provide **policies, training, and safeguards**.
- MPC Volunteers must follow **security rules**.
- MPC remain **legally responsible** for any data breach.
- The user does **not** gain employment rights simply by using their own device for MPC work

1. PURPOSE OF THIS POLICY

This policy sets out how MPC manage the use of **personal devices** by:

- MPC's Clerk (employee).
- Elected or co-opted MPC Councillors.
- Volunteers assisting MPC.

Its purpose is to ensure:

- Compliance with UK GDPR and the Data Protection Act 2018.
- Protection of residents' personal data.
- Clarity about responsibilities and boundaries.
- Protection of individuals' privacy when using their own devices for MPC work.

2. WHO THIS POLICY APPLIES TO

This policy applies to:

- **MPC's Clerk** when using any personal device for council business.
- **MPC Councillors** when accessing or storing council information.
- **MPC Volunteers** when accessing or storing council information.

This policy does **not** change the employment status of any individual. MPC Councillors and Volunteers remain **unpaid office-holders** or **volunteers**, not employees.

3. KEY PRINCIPLES

- MPC are the **data controller** for all personal data processed for MPC purposes.
- Anyone using a personal device for MPC work acts under MPC authority.
- Personal devices remain private; the MPC cannot access personal content.
- MPC may require the deletion of **MPC data only**.
- MPC must be able to comply with data subject requests and data deletion obligations.

4. PERMITTED USE OF PERSONAL DEVICES

Personal devices may be used for:

- Accessing MPC email.
- Reading or drafting MPC documents.
- Participating in online meetings for MPC work.
- Accessing cloud-based systems approved by MPC for MPC data storage.
- Routine MPC administrative tasks

Personal devices **must not** be used to store or process any MPC:

- Special category data (health, ethnicity, political opinions, etc).
- Safeguarding information.
- Confidential HR matters.
- Large datasets containing residents' personal information.
- Electoral roll data (unless explicitly authorised and secured).

If such data is received accidentally, the individual **must** notify MPC's Clerk and delete it immediately.

5. SECURITY REQUIREMENTS

Anyone using a personal device for MPC business must ensure:

5.1 Device Security

- Device is protected by a PIN, password, fingerprint, or facial recognition.
- Operating system and apps are kept up to date.
- The operating system's latest security updates are installed.
- Device encryption is enabled (BitLocker, FileVault, or built-in encryption).
- Automatic screen lock is enabled.

5.2 Data Handling

- MPC data must be stored in approved systems (such as MPC's email system, SharePoint, OneDrive, etc).
- MPC documents must not be stored permanently on the personal device.

- MPC data must not be shared via personal messaging apps (such as WhatsApp, Facebook, Messenger, SMS).
- Public Wi-Fi must not be used for MPC purposes unless the personal device has an active VPN.

5.3 Loss or Theft: If a personal device used for MPC business is lost, stolen, or compromised, the individual must notify MPC's Clerk **immediately**. MPC may require you to remotely delete **MPC data** stored on the device.

6. PRIVACY AND MONITORING

- MPC has **no right** to access personal photos, messages, apps, or files.
- MPC may request deletion of all or some **MPC data,** or revoke access to MPC IT systems.
- If Mobile Device Management (MDM) is used, it will apply only to MPC data containers.

7. EXPENSES

- MPC Councillors and volunteers are **not required** to use personal devices.
- MPC are **not obliged** to reimburse personal device costs, mobile data, or broadband.
- MPC may reimburse reasonable out-of-pocket expenses if pre-approved.
- MPC Clerk's use of personal devices may be reimbursed only if agreed in the MPC Clerk's contract or by MPC resolution.

8. ACCEPTABLE USE

When using a personal device for MPC purposes individuals **must**:

- Use personal devices responsibly and professionally.
- Keep MPC data separate from personal data.
- Report any MPC data breach immediately.
- Avoid downloading MPC documents to unapproved apps.

When using a personal device for MPC purposes individuals **must not**:

- Share devices with others while logged into MPC systems.
- Bypass security controls, included using hacked devices or software.
- Use personal devices for activities that could bring MPC into disrepute.

9. ENDING A ROLE

When a MPC Councillor leaves office, or a volunteer steps down:

- All MPC data that is not in the public domain must be deleted.
- Access to MPC systems will be revoked.
- Any downloaded MPC documents that are not in the public domain must be returned or deleted.
- The individual must confirm deletion if requested.

10. CHANGING A PERSONAL DEVICE OR WORK DEVICE

When a MPC Councillor, or a Volunteer changes a personal device:

- All MPC data that is not in the public domain must be deleted from the redundant personal device.
- The individual must confirm deletion if requested.

When MPC's Clerk changes a work device all data from the MPC Clerk's previous work device must be deleted.

11. POLICY ACCEPTANCE

All MPC Councillors, MPC's Clerk, and specialist Volunteers **must** confirm that they have read, understood, and agree to comply with this policy before using personal devices for MPC business.

PART 3: MAULDEN PARISH COUNCIL BRING YOUR OWN DEVICE (INCLUDING WEBMAIL-ONLY OPTION) DECLARATION

Name: _____

MPC Role (tick one): ☐ Clerk (employee) ☐ Councillor ☐ Specialist Volunteer / Advisor

Personal Device(s) Covered by This Declaration:

1. Acknowledgement of Policy

I confirm that I have received, read, and understood MPC's BYOD Policy, including the Webmail-Only Access Option, and agree to comply with it when using my personal device(s) for MPC **business.**

2. My Chosen Access Method (tick one)

☐ Webmail-Only Access (Low-Risk Mode)

I will access MPC email only through the **MPC-approved** web interface and will not download or store MPC data on my device. I understand that under this option:

- No MPC data that is not in the public domain is stored on my device.
- MPC have no lawful basis to access, search, or wipe my device.
- I must keep my device secure (eg PIN/password, updates, screen lock) when in use for MPC business.

- If I do change to using BOYD access using an email app or download MPC documents, I will inform MPC's Clerk within 24 hours

☐ **Full BYOD Access (Email App/Downloads)**

I will access MPC email using an email app or will download MPC documents. I understand that under this option:

- MPC data may be stored on my device.
- I must comply with MPC's full BYOD security requirements.
- MPC may require deletion of MPC data from my device

3. Data Protection Responsibilities

I understand that:

- MPC are the data controller for all personal data processed for MPC purposes.
- I must follow MPC's data protection, confidentiality, and security rules with respect to MPC data.
- I must report any loss, theft, or compromise of my device used to access MPC data immediately to MPC's Clerk.

4. Privacy And Data Separation

I understand that:

- MPC have no right to access my personal photos, messages, apps, or files.
- MPC may require deletion of MPC data only.
- I must not forward MPC emails to personal accounts or store MPC data that is not in the public domain in personal apps.

5. Ending My Role

I agree that when I leave my MPC role or cease assisting MPC:

- I will delete all MPC data that is not in the public domain from my device(s).
- I will return or destroy any downloaded MPC documents that are not in the public domain.
- I will confirm deletion if requested.

6. Voluntary Use Of Personal Devices

I understand that:

- I am not required to use my personal device for MPC business.
- MPC are not obliged to reimburse device costs unless agreed in advance.

Signature

I agree to comply with MPC's BYOD Policy:

Signed: _____

Name: _____

Date: _____

MPC Officer Receiving Form: _____