Lytchett Matravers Parish Council

Bring Your Own Device (BYOD) Policy

1. Purpose

This policy sets out the rules and expectations for councillors, employees, and authorised contractors who wish to use their own personal devices (such as laptops, tablets, and smartphones) to access Parish Council information, systems, and communications.

The aim is to support flexible working while ensuring that Parish Council data is kept secure and in compliance with legal and regulatory requirements.

2. Scope

This policy applies to:

- All councillors, employees, and contractors of Lytchett Matravers Parish Council who access Council information using personal devices.
- All personal devices used for Council business, including laptops, smartphones, and tablets.
- Access to Parish Council email accounts, documents, and any other data held electronically.

3. General Principles

- Use of personal devices for Council business is **voluntary**. The Council does not require anyone to use their own equipment.
- Users must ensure their personal devices are **secure, up to date, and protected** against unauthorised access.
- The Parish Council reserves the right to restrict or remove access to Council systems if security concerns arise.

4. Security Requirements

Anyone using their own device for Council business must:

1. Use a **password or PIN** to lock the device.
2. Ensure the device has up-to-date **antivirus and security software** (where applicable).
3. Keep the operating system and applications updated with the latest security patches.
4. Not share their device with others when accessing Council data.
5. Immediately report to the Parish Clerk any **loss, theft, or suspected compromise** of a device used for Council work.
6. Allow the Clerk (or nominated IT support provider) to require changes if a device is found not to meet minimum security standards.

5. Data Protection and Privacy

- Parish Council information must only be stored in **approved systems** (e.g., Council email, cloud storage provided by the Council). It should not be stored locally on personal devices unless absolutely necessary.
- All users must comply with the **UK GDPR** and **Data Protection Act 2018** when handling Council data.
- Personal devices may be subject to inspection if required for legal, regulatory, or data protection reasons.
- Personal data belonging to the user (such as photos, contacts, or personal emails) will not be accessed by the Council unless required by law.

6. Use of Email and Communications

- Council email accounts must be used for all official correspondence. Personal email accounts must not be used for Council business.
- Sensitive or confidential information must not be downloaded or stored on personal devices unless authorised and protected.

7. Responsibilities of the Council

- The Parish Council will provide secure access to its systems for BYOD users where appropriate.
- The Council will offer guidance and reasonable support on security requirements but is **not responsible for costs** associated with purchasing, maintaining, or repairing personal devices.
- In the event of loss, theft, or breach, the Council may require a remote wipe of Council-related data from the device.

8. Enforcement

Failure to comply with this policy may result in:

- Withdrawal of BYOD access.
- A report to the Monitoring Officer (for councillors).
- Disciplinary action (for employees or contractors).
- Notification to the Information Commissioner's Office (ICO) in the event of a data breach.

9. Review

This policy will be reviewed **annually** or sooner if legislation, technology, or security risks change.

Adopted by Lytchett Matravers Parish Council: Full Council 25th February 2026

Minute Reference: 5.3

Next Review Due: March 2027