IT Policy

1. Purpose

This policy sets out how Lytchett Matravers Parish Council will manage its information technology systems, safeguard data, and ensure compliance with legal and financial responsibilities under Assertion 10 of the AGAR, which requires that the Council has proper arrangements in place to safeguard public money, assets, and information.

2. Scope

This policy applies to all councillors, employees, and authorised contractors who use Parish Council IT systems, data, or equipment, including:

- Council-owned computers, laptops, tablets, and phones.
- Council email and cloud storage accounts.
- Any personal devices used for Council business (BYOD – Bring Your Own Device).

3. Principles

3.1 Security of IT Systems

- All devices must be password protected with strong, unique passwords.
- Devices must have up-to-date antivirus and security patches installed.
- Remote access to Council data is permitted only via secure, encrypted connections.
- Any suspected breach of IT security must be reported to the Parish Clerk immediately.

3.2 Data Protection & Privacy

- The Council will comply with the Data Protection Act 2018 and UK GDPR.
- Personal data will only be collected, stored, and processed when necessary for Council business.
- Access to personal data will be restricted to those who need it for their role.
- Data will be stored in secure cloud-based services with multi-factor authentication where available.

3.3 Financial & Governance Integrity

- Financial data, bank access, and accounting records will be stored securely and backed up regularly.
- Only authorised personnel will have access to financial systems and online banking.
- All changes to financial systems or IT security settings will be logged.

3.4 Backup & Business Continuity

- All essential Council documents and financial records will be backed up at least weekly.
- Backups will be stored securely off-site or in a secure cloud service.
- A continuity plan will ensure that in the event of equipment failure, data breach, or cyber incident, Council business can resume promptly.

3.5 Email & Communication

- Councillors and staff must use their official Council email addresses for Council business.
- Council email accounts will be archived in line with the Council's Document Retention Policy.
- Sensitive information must not be sent via unsecured or personal accounts.

3.6 Personal Devices

- Where personal devices are used for Council business, they must comply with the same security standards as Council-owned equipment.
- Council data must be stored separately from personal data where possible.

3.7 Disposal of IT Equipment

- Before disposal, all devices will be securely wiped of Council data.
- IT equipment will be disposed of in an environmentally responsible way.

4. Training & Awareness

- All councillors and staff will be briefed on cyber security awareness at least annually.
- Updates on emerging threats and best practices will be shared as necessary.

5. Monitoring & Review

- This policy will be reviewed annually alongside other governance documents.
- The Parish Clerk will monitor compliance and report any breaches to the Council.

Adopted by Lytchett Matravers Parish Council: 24th September 2025
Minute Reference: 12 – 24.9.25
Reviewed at Full Council, 25th February 2026
Minute ref: 5.3

Next Review Due: March 2027