Marldon Parish Council IT Policy

1. Purpose and Scope

This policy sets out how Marldon Parish Council manages and protects its information technology (IT) systems, data, and electronic communications.

It applies to all Councillors, staff, contractors, and volunteers who use Council IT equipment, systems, or data, whether on Council-provided devices or personal devices used for Council business.

2. Principles

- **Confidentiality** – Information is accessed only by those who need it.
- **Integrity** – Data is accurate, complete, and protected against misuse or corruption.
- **Availability** – IT systems and data remain available to support Council business.
- **Accountability** – Users are responsible for their actions when using Council IT.
- **Compliance** – The Council complies with all relevant UK laws, including the **UK GDPR**, **Data Protection Act 2018**, **Freedom of Information Act 2000**, and **Computer Misuse Act 1990**.

3. Acceptable Use

- Council IT systems and email accounts must be used for Council business.
- Limited personal use is acceptable, provided it does not interfere with Council duties, incur costs, or breach security.

4. Information Security

- **Passwords**: Must be strong (12+ characters with a combination of uppercase letters, lowercase letters, numbers, and symbols.) and not shared. Multi-factor authentication should be used where available.
- **Data Protection**: Personal data must only be stored, shared, and retained in line with the Council's Data Protection Policy.
- **Email Security**: Use Council provided email accounts for Council business; do not forward confidential emails to personal accounts.
- **Devices**: All devices used for Council business must be password/PIN protected and kept up to date with security patches.

5. Data Management and Storage

- Official documents must be stored in Council-approved systems (e.g., secure cloud storage or encrypted devices).

- Personal devices used for Council business must use secure storage with disk encryption enabled
- Data must not be stored on unencrypted USB sticks or personal cloud accounts.
- Backups must be performed regularly and tested.

6. Internet and Email

- Personal email accounts should not be used.
- Users must be vigilant against phishing and malicious websites.
- Large attachments or sensitive data must be shared securely (e.g. encrypted files or secure file transfer services).

7. Email Data Retention

- **Retention Periods**:
  - Routine correspondence: retained for **up to 1 year**, unless required longer for ongoing Council business.
  - Formal Council business (e.g., agendas, minutes, financial records, contracts, or legal matters): retained in line with the Council's **Records Retention Policy** (typically 6–7 years, or permanently for key governance documents).
  - Personal data: kept only as long as necessary for the purpose it was collected, then securely deleted.
- **Storage & Archiving**:
  - Emails that form part of the official Council record must be saved into the Council's secure document management system (e.g., cloud storage or shared drive).
  - Councillors and staff should **not** rely on their inbox as a permanent record-keeping system.
- **Deletion**:
  - At the end of the retention period, emails will be securely deleted.
  - Users must regularly review and clear their inboxes, ensuring important records are properly archived first.

8. Incident Management

- Any suspected data breach, or loss/theft of a device containing Council data such as emails must be reported immediately to the Clerk or designated IT contact.
- The Council will investigate and, where required, notify the Information Commissioner's Office (ICO) within 72 hours of any data breach.

9. Social Media and Communications

- Councillors and staff must distinguish between personal and official accounts.
- Official social media accounts must be managed responsibly, with appropriate controls on access.
- Confidential information must not be shared on public platforms.

10. Training and Awareness

- All users must undertake periodic training in data protection, cybersecurity, and safe IT use.
- The Council will review this policy annually and update it in line with best practice.

11. Compliance and consequences

- Breach of this IT and Email Policy may result in the suspension of IT privileges and
  further consequences as deemed appropriate.

12. 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