NEWPORT PARISH COUNCIL

Newport Parish Council – IT Policy

1. **Purpose**

This IT Policy sets out the principles and procedures for the use, management, and security of IT resources owned by Newport Parish Council. It ensures data integrity, compliance with relevant laws (including GDPR), and supports effective operation of council duties.

2. Scope

This policy applies to:
- The Parish Clerk/RFO, who is the sole user of council-owned IT equipment.
- All councillors, regarding access to information, communications, and use of their own devices for council business.

3. IT Equipment

- The council owns one laptop used solely by the Clerk/RFO for official business.
- This equipment must be kept secure and protected with strong passwords and encryption.
- No unauthorised software is to be installed, and all software must be kept up to date.
- A regular back up of all data will be completed by the Clerk/RFO to an external hard drive.
- The Chair will have a separate back up copy of the Parish documents – backed up twice yearly.

4. Data Management

- All council documents must be stored in a secure and backed-up system (e.g., encrypted cloud storage or secure local backup).
- Data must be retained and disposed of in accordance with the council's Document Retention Policy and relevant data protection regulations.

5. Email and Communications

- The Clerk/RFO must use a dedicated parish council email address (e.g., clerk@newportparish.gov.uk).
- Councillors are expected to use secure email accounts when corresponding about council business.
- Sensitive data must not be shared via unsecured email or messaging apps.

6. Website Management

- The Clerk is responsible for updating and maintaining the council's website to ensure compliance with accessibility regulations and transparency obligations (e.g., publication of minutes, agendas, financial documents).
- Website content must be accurate, timely, and non-partisan.

7. Security and Access

- The council laptop must be password-protected, and antivirus software should be installed and regularly updated.
- Remote access must be secure, using encrypted connections where necessary.

- The Clerk is responsible for ensuring no unauthorised persons use the council-owned device.
- The Clerk must shut down the computer at the end of every work session.

8. Social Media and Public Communication

- If the council uses social media, posts should be factual, non-political, and in line with the council's Communications Policy.
- The Clerk may post updates on behalf of the council with prior approval where required.

9. Councillor Responsibilities

- Councillors must respect confidentiality and handle all council data in accordance with data protection laws.
- Personal devices used for council business should be protected with a password or PIN and secure from unauthorised access.

10. Breach and Enforcement

- Any suspected breach of this policy must be reported to the Chair of the Council.
- Breaches may result in further investigation and appropriate action, in line with council procedures.

11. Review and Monitoring

This policy will be reviewed every year or earlier if significant changes occur in technology, regulations, or council operations.

Approved by Newport Parish Council on 8th July 2025
Minute Reference: 2025 07 08
Next Review Due: July 2026