YEOVIL WITHOUT
PARISH COUNCIL

IT Policy

Adopted: 18 March 2026 | Review Due: May 2027

1. Introduction

Yeovil Without Parish Council is a small parish council with one member of staff:

- The Parish Clerk - the sole officer with access to council IT systems

This policy reflects the council's size, limited IT use, and proportionate level of risk. It has been prepared to support compliance with Assertion 10 of the Annual Governance and Accountability Return (AGAR), which requires councils to demonstrate that appropriate arrangements are in place to manage cyber security and information risk.

2. Purpose of the Policy

The purpose of this IT Policy is to:

- Protect the council's information and digital assets
- Ensure IT systems are used safely, securely, and lawfully
- Reduce the risk of data loss, cyber incidents, or unauthorised access
- Demonstrate good governance and compliance with statutory requirements

3. Scope

This policy applies to:

- The Parish Clerk
- Councillors, where they are provided with or granted access to council IT systems (such as council email accounts)

4. IT Systems in Use

The council's IT provision includes:

- A council-owned computer used by the Clerk
- A .gov.uk website
- .gov.uk email accounts
- Cloud-based document storage and backup services (where applicable)

Only the Clerk is authorised to access and manage these systems unless the council formally resolves otherwise.

5. Roles and Responsibilities

The Clerk is responsible for:

- Day-to-day operation of council IT systems
- Maintaining the security of devices, accounts, and data
- Applying software and security updates promptly
- Managing passwords and access controls
- Reporting any IT or data security incidents to the Chair of Council

The council is responsible for:

- Approving and reviewing this policy
- Ensuring proportionate cyber security arrangements are in place

6. Acceptable Use

Council IT equipment and systems are provided for council business only.
The Clerk must:

- Use IT systems responsibly and professionally
- Not install unauthorised software or hardware
- Lock devices when unattended
- Ensure confidential information cannot be accessed or viewed by unauthorised persons

Limited personal use is discouraged and must not interfere with council business.

7. Home and Remote Working

Where the Clerk works from home or remotely (whether regularly or occasionally), the following controls apply:

- Council IT equipment must be kept secure at all times
- Screens must not be visible to other household members or visitors
- Paper records must be stored securely and disposed of appropriately
- Council data must not be accessed using public or unsecured Wi-Fi
- Extra care must be taken when working in public places to prevent unauthorised access to information

8. Email and Internet Use

- Only council-issued .gov.uk email accounts must be used for council business
- Personal email accounts must not be used for council correspondence
- Emails should be treated as formal council records where appropriate
- Care must be taken to avoid phishing emails, suspicious links, or attachments.

The council website must be:

- Accessed securely
- Maintained using strong passwords
- Updated only with lawful, accurate, and appropriate content

9. Passwords and Security

- Strong passwords must be used in line with National Cyber Security Centre (NCSC) guidance
- Passwords must not be shared
- Multi-Factor Authentication (MFA) must be enabled where available
- Devices must be protected with a password or PIN Passwords must be changed immediately if compromise is suspected.

10. Data Protection and Backups

- All personal data must be processed in accordance with the UK GDPR and the council's Data Protection Policy
- Council data must be stored securely
- Regular backups must be in place, such as automatic cloud backups
- Council data must not be stored unnecessarily on personal devices

11. Cyber Incidents and Reporting

Any actual or suspected:

- Data breach
- Loss or theft of equipment
- Email or account compromise
- Cyber attack or malware incident

must be reported immediately to the Chair and investigated promptly.

Where required, incidents will be reported to the Information Commissioner's Office (ICO).

12. Review and Approval

This policy will be:

- Reviewed at least annually
- Updated where there are changes to technology, legislation, or risk

This policy supports compliance with AGAR Assertion 10 by confirming that the council has considered cyber security risks and put proportionate controls in place.

Document Control

Title: IT Policy

Owner: Yeovil Without Parish Council

Created: Mar 2026

Approved: 18 Mar 2026 (Minute Ref: 544/26.1)

Review annually at the annual parish council meeting held in May