Upchurch Parish Council

Clerk to the Council:
Mrs N Henley

e-mail: clerk@upchurchparishcouncil.gov.uk

Document Control

Title	IT Policy
Document Type	Governance
Author	Clerk
Owner	Upchurch Parish Council
Subject	IT
Created	Feb 2026
Approved by	Full Council
Date Approved	05 Feb 2026
Minute Reference	472-FCM/02/26 III
Review Date	Feb 2027

IT POLICY

1. Introduction

Upchurch Parish Council is a small parish council with **one member of staff**, the Parish Clerk. The Clerk works primarily **from home** and is the **only person with access to council IT systems**.

This policy reflects the council's size, home-working arrangements, and limited but essential use of digital systems. It has been prepared to meet the requirements of **Assertion 10 of the Annual Governance and Accountability Return (AGAR)**, confirming that the council has appropriate and proportionate arrangements in place to manage cyber 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)

No other staff or contractors have access to council IT systems unless formally authorised by the council.

4. IT Systems in Use

The council’s IT provision includes:

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

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

5. Roles and Responsibilities

Parish Clerk

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 Chairman

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 others in the home environment

7. Home and Remote Working

As the Clerk works from home, the following controls apply:

- Council equipment must be kept in a secure location within the home
- Screens must not be visible to family 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
- Care must be taken when working in public places to prevent unauthorised viewing or access

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
- Suspicious emails, links, or attachments must not be opened and should be deleted or reported

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 should 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 Chairman 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.