Hartlip Parish Council

Clerk to the Council:
Mr C Henley

e-mail: clerk@hartlippc.gov.uk

Document Control

Title	IT Policy
Document Type	Governance
Author	Clerk / Full Council
Owner	Hartlip Parish Council
Subject	Information Technology
Created	January 2026
Approved by	Full Council
Date Approved	11 February 2026
Minute Reference	498.FCM/02/26.II/III
Review Date	March 2027

1. Introduction

Hartlip Parish Council is a small parish council with one member of staff:

- The Parish Clerk who primarily works from home (the sole officer with access to council IT systems).

This policy has been written to reflect the council's size, limited IT use, and proportionate risk, while meeting the requirements of Assertion 10 of the Annual Governance and Accountability Return (AGAR), which confirms that the council has appropriate policies, procedures, and controls 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 safe and lawful use of IT systems
- Reduce the risk of data loss, cyber attack, or misuse
- Demonstrate compliance with good governance and data protection requirements

3. Scope

This policy applies to:

- The Parish Clerk
- Councillors, where they are provided with or granted access to council IT systems (e.g. email)

4. IT Systems in Use

The council's IT provision is limited and includes:

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

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

5. Roles and Responsibilities

Parish Clerk

The Clerk is responsible for:

- Day-to-day operation of council IT systems
- Ensuring security updates are applied
- Managing passwords and access controls
- Reporting any IT or data security incidents to the Chairman

Council

The council is responsible for:

- Approving this policy and reviewing it regularly
- Ensuring proportionate arrangements are in place to manage cyber risk

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 the computer when unattended
- Ensure confidential information is not visible to unauthorised persons

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

7. 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 records and retained where required
- Care must be taken to avoid phishing, suspicious links, or attachments

The council website must be:

- Maintained securely
- Updated using strong passwords
- Used only for lawful and accurate content

8. Passwords and Security

- Strong passwords must be used at all times (in line with National Cyber Security Centre 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 should be changed immediately if compromise is suspected.

9. Data Protection and Backups

- All personal data must be handled 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 (automatic cloud backup or equivalent)
- Data must not be stored unnecessarily on personal devices

10. Remote Working

Where the Clerk works from home:

- Council equipment must be used wherever possible
- Screens should not be visible to others
- Documents must be stored securely
- Public or unsecured Wi-Fi should be avoided

11. Cyber Incidents and Reporting

Any actual or suspected:

- Data breach
- Loss or theft of equipment
- Cyber attack or email compromise

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 in response to changes in technology, risk, or legislation

This policy supports the council's compliance with AGAR Assertion 10 by demonstrating that appropriate and proportionate cyber security arrangements are in place.