

Over Haddon Parish Council

IT and Acceptable Use Policy

Adopted: [11/5/26]

Review Date: Two years from adoption

1. Purpose

To ensure secure, lawful and effective use of Council IT systems and protect Council data.

2. Scope

Applies to the Council laptop, email accounts, digital records, and any personal devices used for Council work. Only the Clerk or Acting Clerk may use the Council laptop unless authorised.

3. Responsibilities

The Clerk manages secure use, passwords, backups, and incident reporting. The Council ensures compliance and provides appropriate systems.

4. Acceptable Use

Use is primarily for Council business. Limited personal use is acceptable if low risk. Illegal, offensive, or unsafe use is prohibited.

5. Security

- Strong passwords and screen locking required
- Device stored securely at all times
- Antivirus and updates must be current

6. Data Protection

All handling of personal data must comply with UK GDPR. Only necessary data should be accessed and securely stored.

7. Email and Cyber Awareness

Be alert to phishing emails, suspicious links, and unexpected attachments. Never share passwords or sensitive data via email.

8. Backup and Storage

Council data must be regularly backed up. Important records must not be stored in a single location only.

9. Personal Devices

If used, devices must be password protected and Council data deleted when no longer needed.

10. Data Breach Procedure

Any loss, breach, or suspected cyber incident must be reported immediately to the Chair.

The Council will assess and report to the ICO where required.

11. Business Continuity Access

The Council may access systems where necessary for continuity, absence, or investigation.

12. Ending Access

On leaving role, all equipment must be returned and access credentials handed over or

reset. **13. Policy Review**

Reviewed every two years or sooner if legislation or risks change.

Signed:

Chair of the Council _____ Zena Hawley _____ Date: _____

Parish Clerk _____ Zena Hawley _____ Date: _____