Highley Parish Council – IT, Digital Governance & AI Policy (2026 Update)

To be adopted at the Full Council Meeting – 12 May 2026

1. Purpose

This policy sets out Highley Parish Council's approach to:

- Secure and lawful use of IT systems
- Digital governance and data handling
- Cybersecurity and device management
- Use of Artificial Intelligence (AI) tools
- Compliance with **Assertion 10 (SAPPP 2025)**

The aim is to ensure that all digital activity undertaken by or on behalf of the Council is **secure, transparent, accountable and compliant** with statutory requirements.

2. Scope

This policy applies to:

- Councillors
- The Clerk/RFO
- Employees
- Contractors and volunteers handling Council information
- Anyone using Council IT systems, devices, email accounts or digital platforms

It covers the use of:

- Council-owned devices
- Personal devices used for Council business
- Email and communication systems
- Cloud storage and digital records

- AI tools (e.g., Microsoft Copilot)
- Social media and online platforms

3. Principles of Digital Governance

Highley Parish Council operates under the following principles:

3.1 Transparency

Digital systems must support open governance, compliance with the Transparency Code, and publication of required information.

3.2 Accountability

All decisions and outputs remain the responsibility of the Clerk and elected members, regardless of digital tools used.

3.3 Security

All IT systems must be used in a way that protects Council data, devices and networks.

3.4 Ethical Use

Technology must support—not replace—human judgement, especially in discretionary or sensitive matters.

3.5 Compliance

All digital activity must comply with:

- UK GDPR
- Data Protection Act 2018
- Freedom of Information Act 2000
- Local Government legislation
- SAPPP Assertion 10 requirements

4. IT Systems & Device Management

4.1 Council-Owned Devices

- Council devices are for **official use only**.
- Devices must not be altered, dismantled or have unauthorised software installed.
- Devices must be kept secure, clean and protected from damage.
- Loss or theft must be reported immediately.
- All Council devices must be returned when a role ends.

4.2 Personal Devices

Personal devices **must not** be used for storing or processing Council data unless explicitly authorised.

Where authorised:

- No Council data may be stored unencrypted.
- No Council data may be stored in personal cloud accounts.
- Devices must be password-protected and secured.
- Cached files and downloads must be deleted after use.
- The Council may require temporary access to retrieve Council data in legal or audit situations.

5. Email & Communication Protocols

5.1 Official Email Accounts

- All Council business must be conducted using **official Council email addresses**.
- Forwarding Council emails to personal accounts is prohibited.
- Personal use of Council email accounts is not permitted.

5.2 Email Security

- Be cautious with attachments and links.
- Verify sender identity before opening unexpected content.
- Sensitive information must not be emailed without encryption.

- Emails containing personal data must be deleted when no longer required.

5.3 Communication Standards

- Emails must be professional, respectful and compliant with the Code of Conduct.
- Email must not replace necessary face-to-face or telephone communication.

6. Passwords & Access Control

Highley Parish Council follows **NCSC guidance**:

6.1 Password Requirements

- Passwords must use the **three random words** method (e.g., *RiverLampOrange*).
- Passwords must not be shared.
- Default passwords must be changed immediately.
- Administrative passwords must be stored securely, with a sealed emergency copy held by the Chair.

6.2 Multi-Factor Authentication (MFA)

MFA must be enabled wherever possible.

6.3 Account Management

- Access is removed immediately when a role ends.
- Attempts to access unauthorised accounts will be treated as a security incident.

7. Data Protection & Digital Records

7.1 Data Storage

- Council data must be stored only on approved systems.
- Personal data must not be stored on personal devices or unapproved cloud services.
- Backups must be maintained in line with Council procedures.

7.2 Subject Access Requests (SARs)

The Council maintains a SAR procedure ensuring:

- Requests are acknowledged and completed within statutory timeframes
- Data is provided securely
- Exemptions are applied lawfully
- Records of SARs are maintained

7.3 Website & Accessibility

The Council will:

- Maintain a compliant website meeting **WCAG 2.2 AA** standards
- Publish all required documents (minutes, AGAR, councillor details, policies)
- Conduct periodic accessibility and link-checking audits

8. Cybersecurity

8.1 Core Requirements

- Anti-virus and security updates must be enabled.
- Devices must be locked when unattended.
- Portable devices must not be left in vehicles or unsecured locations.
- Council data must not be stored on removable media unless encrypted.

8.2 Reporting Incidents

All suspected breaches must be reported immediately to the Clerk (or Chair if the Clerk is affected).

8.3 Remote Working

When working remotely:

- Screens must not be visible to others.
- Printed documents must be stored securely.
- Council data must not be left unattended.

- Devices must be logged out after use.

9. Use of Artificial Intelligence (AI)

Highley Parish Council uses AI tools (e.g., Microsoft Copilot) to support administrative efficiency.

9.1 Principles

- AI supports but does not replace human decision-making.
- All AI-generated content must be reviewed by the Clerk or relevant councillor.
- AI must not be used for:
    - Legal interpretation
    - Disciplinary decisions
    - Safeguarding decisions
    - Determining eligibility for services
- AI must not be used to process sensitive personal data.

9.2 Security

- AI tools may only be accessed through secure, licensed platforms provided by Wavenet.
- No personal data may be entered into AI tools unless compliant with UK GDPR.

10. Social Media & Online Conduct

10.1 Official Council Channels

Only the Clerk or Chair may post on official Council social media pages unless delegated.

10.2 Personal Use

Councillors and staff must:

- Not imply they speak for the Council
- Not disclose confidential information
- Not post content that could be discriminatory, defamatory or damaging to the Council
- Follow the Code of Conduct at all times

10.3 Content Restrictions

The following must never be posted:

- Personal data
- Confidential documents
- Internal discussions
- Information relating to grievances, disciplinary matters or legal issues

11. Monitoring & Compliance

11.1 Monitoring

The Council may monitor:

- Email usage
- Internet activity
- Council data stored on personal devices (where authorised)

Monitoring will be:

- Necessary and proportionate
- Conducted in line with UK GDPR
- Logged and reviewed appropriately

11.2 Misuse

Misuse of IT systems may result in:

- Withdrawal of IT access
- Disciplinary action
- Referral to external authorities (e.g., ICO, Police)

12. Training

The Council will provide:

- Annual IT and cybersecurity training
- Data protection and SAR training

- AI use guidance
- Induction training for new councillors and staff

13. Review

This policy will be reviewed:

- Annually at the Annual Council Meeting
- Following major technological or legislative changes
- After any significant incident

14. Adoption

This IT, Digital Governance & AI Policy is adopted by Highley Parish Council on:

12 May 2026 at the **Full Council Meeting**.