

Parish Council IT & Data Compliance Policy

1. Purpose

To ensure secure, transparent, and legally compliant use of digital systems and personal data, in line with the new **Assertion 10** requirement—formerly part of Assertion 3—in the Annual Governance Statement (AGS) and Annual Governance and Accountability Return (AGAR) effective from FY 2025/26

2. Scope

Applies to all parish councillors, staff, volunteers, contractors, and third parties who use, manage, or support the Council's IT systems or process personal data.

3. Council-Owned Domain & Email

- All official communications must use a **generic email address** hosted on a **council-owned domain**, e.g., clerk@yourcouncil.gov.uk or .org.uk. Personal or free email services (Gmail, Hotmail, etc.) are prohibited
- The domain should ideally be .gov.uk for enhanced credibility and security; .org.uk is acceptable

4. Website Management & Accessibility

- Maintain a council website that complies with **WCAG 2.2 AA** and the **Public Sector Bodies Accessibility Regulations 2018**, ensuring ongoing accessibility
- Publish required documentation as mandated by the **Freedom of Information Act 2000** and the **Transparency Code for Smaller Authorities**, as appropriate

5. Data Protection & Compliance

- Comply fully with the **UK GDPR** and **Data Protection Act 2018**, recognizing the Council's role as both **Data Controller** and **Data Processor**
- Personal data must be processed lawfully, fairly, and transparently, with clear understanding of:
 - Purpose and lawful basis for processing
 - Storage location and retention periods
 - Access permissions
 - Sharing and data deletion protocols

6. Technical and Organisational Measures

- Implement appropriate **technical controls** (e.g., strong access controls, antivirus/anti-malware, encrypted backups) and **organisational measures** (e.g., secure data handling, access logs) to safeguard personal data
- Conduct **data audits** regularly to document data flows and assess risk

7. IT Usage & Security

- Define usage guidelines for **council-owned equipment** and **personal devices** (if permitted), covering:
 - Secure password use
 - Encryption requirements
 - Safe network practices
 - Approval and support processes.

8. Training and Awareness

- Require all councillors and staff to undertake **regular training** on:
 - UK GDPR and Data Protection Act 2018
 - FOI obligations
 - IT security best practices
 - Council's IT policy and procedures

9. Record-Keeping & Audit Trail

- Maintain accurate records of:
 - Data audit findings
 - Policy approvals (via Council minutes)
 - Training attendance
 - Security incidents and remedial actions.

10. Policy Approval & Review

- The policy must be approved by **full council**, minuted formally, and reviewed **annually**, or sooner if there are legislative, technological, or operational changes.

Rationale & Alignment with Assertion 10

From FY 2025/26, **Assertion 10: Digital and Data Compliance** becomes a mandatory part of the AGS and AGAR. To warrant a positive response under AGS Assertion 10, a council must implement the following:

- Use of council-owned domain and email systems
- Accessible and transparent web presence
- Data protection measures under UK GDPR and DPA 2018
- Recognition of controller/processor roles
- Adoption of a formal IT policy governing secure practices

This policy aligns with these requirements and provides a clear framework for ensuring ongoing compliance.
