# Assertion 10 – Digital & Data Compliance

- A Practical Guide for Town and Parish Councils

www.calc.org.uk

**Introduction**
Assertion 10 is a new requirement introduced in the 2025 Practitioners' Guide for smaller authorities. It applies to Annual Governance and Accountability Returns (AGAR) for the financial year beginning 1st April 2025.

This assertion ensures that councils demonstrate real compliance with digital and data protection matters — not just good intentions. It places legal and practical obligations on councils relating to:

- Email management
- Website compliance
- Personal data handling
- IT policies

**What Councils Must Do**
**Email Management**

- Councils must use a generic email account on a domain owned by the authority.
    - Acceptable
      clerk@abcparishcouncil.gov.uk, clerk@abcparishcouncil.org.uk, clerk@abcparishcouncil.co.uk, clerk@abcparishcouncil.com etc.
    - Not acceptable
      abcparishclerk@gmail.com or abcparishclerk@outlook.com
- Dedicated council-owned emails should be issued to councillors and staff.

**Accessible & Compliant Website**
Councils (excluding parish meetings) must ensure their website complies with:

- Web Content Accessibility Guidelines (WCAG) 2.2 AA
- Public Sector Bodies (Websites & Mobile Applications) Accessibility Regulations 2018
- Freedom of Information Act 2000 (required publications)
- Transparency Code for Smaller Authorities (where applicable)

Practical steps:

- Publish FOI and Transparency Code documents on the website.
- Provide an up-to-date accessibility statement.
- Regularly test the website against WCAG 2.2 AA standards.

**Personal Data & GDPR**
All authorities (including parish meetings) must comply with:

- UK GDPR (2016)
- Data Protection Act (2018)

Councils are both:

- Data Controllers – deciding what data to collect and why.
- Data Processors – handling and storing data securely.

Seven principles of GDPR:
1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability

Practical actions:

- Ensure registration with the Information Commissioner's Office (ICO).
- Adopt and maintain GDPR policies.
- Train councillors and staff in data handling responsibilities.

***Example Template: GDPR Privacy Notice***

This council collects and uses personal data in accordance with the UK GDPR and Data Protection Act 2018. We process data for the following purposes:

- To deliver public services
- To respond to enquiries and complaints
- To manage council staff and councillors
- To comply with legal and financial requirements

Personal data will be stored securely and retained only as long as necessary. For further details, please see our Data Protection Policy.

**IT Policy**

All smaller authorities (except parish meetings) must adopt an IT policy covering:

- Secure use of IT equipment (council-owned and personal devices).
- Responsibilities of clerks, councillors, and staff.
- Procedures for safe use of email, file storage, and software.
- Data security and breach response.

***Example Template: IT Policy (Outline)***

1. Purpose – To set out how councillors and staff should use IT securely.
2. Scope – Applies to all council devices and personal devices used for council business.
3. Email – Council email accounts must be used for all business.
4. Data Security – Use of strong passwords, antivirus software, and secure storage.
5. Personal Devices – Must follow same standards as council devices.
6. Breach Response – All breaches must be reported to the Clerk and ICO where required.

**Next Steps for Councils**

- Audit current compliance against each requirement.
- Register (or confirm registration) with the ICO.
- Upgrade websites to WCAG 2.2 AA standards.
- Migrate email accounts to a council-owned domain.
- Draft and approve an IT policy.
- Review and adopt GDPR-related policies.

**Conclusion**

Assertion 10 introduces a higher standard of accountability for councils in managing digital systems and data. By acting now, councils can:

- Avoid legal or regulatory risks.
- Improve transparency and accessibility for residents.
- Build trust by demonstrating good governance in the digital age.

**Checklists**

***Checklist: Email Management***

Does the council use a domain it owns (e.g., .gov.uk or .org.uk)?
Does every councillor and staff member have a council email address?
Are personal accounts avoided for council business?

***Checklist: Website Compliance***

Accessibility statement published and updated.
Website tested against WCAG 2.2 AA.
All FOI documents are available online.
Transparency Code requirements published.

***Checklist: Data Protection***

Registered with the ICO.
GDPR policy adopted by council.
Staff and councillors trained in data protection.
Privacy notices published.
Data retention schedule in place.

***Checklist: IT Policy***

IT policy formally adopted by the council.
Policy covers use of both council and personal devices.
Guidance on passwords, backups, and encryption.
Data breach response plan included.