

Long Man Parish Council meeting 14 July 2025

Extracts from the revised Practitioner's Guide 2025 relating to Digital and Data Compliance : document pages 14-15 and 46 refer.

Assertion 10 - Digital and data compliance (Assertion 10 added to clarify data compliance, previously covered under Assertion 3)

Note: Assertion 10 will not appear on the AGAR until 2025-26 To warrant a positive response to this assertion, the authority needs to have taken the following actions:

1.47 Email management - Every authority must have a generic email account hosted on an authority owned domain, for example clerk@abcparishcouncil.gov.uk or clerk@abcparishcouncil.org.uk rather than abcparishclerk@gmail.com or abcparishclerk@outlook.com for example.

1.48 All smaller authorities (excluding parish meetings) must meet legal requirements for all existing websites regardless of what domain is being used.

1.49 All websites must meet the Web Content Accessibility Guidelines 2.2 AA and the Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018 (where applicable).

1.50 All websites must include published documentation as specified in the Freedom of Information Act 2000 and the Transparency code for smaller authorities (where applicable).

1.51 All smaller authorities, including parish meetings, must follow both the General Data Protection Regulation (GDPR) 2016 and the Data Protection Act (DPA) 2018.

1.52 All smaller authorities, including parish meetings, must process personal data with care and in line with the principles of data protection.

1.53 The DPA 2018 supplements the GDPR and classifies an authority as both a Data Controller and a Data Processor.

1.54 All smaller authorities (excluding parish meetings) must also have an IT policy. This explains how everyone - clerks, members and other staff - should conduct authority business in a secure and legal way when using IT equipment and software. This relates to the use of authority-owned and personal equipment.

AGS Assertion 10 — Digital and data compliance

5.117. Data protection and security - Using authority-owned email accounts ensures that sensitive information is handled in a controlled environment with appropriate security measures. This aligns with GDPR principles such as data minimisation, integrity and confidentiality.

5.118. Accountability and transparency - authority-owned email accounts provide a clear record of communications, which is essential for transparency and accountability. This helps in maintaining an audit trail and ensures all authority-related communications are accessible for review if needed.

5.119. Consistency, trust and professionalism - it is best practice to use .gov.uk domains for smaller authorities' emails and websites (excluding parish meetings). This helps maintain a consistent and professional image for the authority and ensures all communications are easily identifiable as coming from the authority. This is increasingly important as cyber scams are on the rise. For support on setting up a gov.uk domain for your smaller authority you can follow the guidance on moving your parish council to a .gov.uk domain.

5.120. Having authority-owned email accounts also makes Data Subject Access and Freedom of Information Requests easier to manage.

5.121. Compliance with policies - All authorities should have an IT policy that mandates the use of authority-owned email accounts for official business. These policies are designed to ensure that all communications are conducted in a manner that is consistent with the authority's standards and legal obligations

5.122. IT Policies - An IT policy prevents misunderstandings when using IT equipment for authority business and makes sure that there can be no excuses for anyone in your authority not protecting their data or working safely. If your authority does not have a policy, you might like to use this IT policy template. It is important to personalise the template for the specific use of your authority and add links to guidance where needed.

5.123. Website accessibility - Where a smaller authority is subject to the requirements of website accessibility it does not have to buy a new website to comply with accessibility law if it places a disproportionate burden on the authority. At a minimum all authorities' websites must include an accessibility statement on their website and keep it under regular review. This statement should include reasons for not meeting accessibility requirements, ways to source alternative copies of non-accessible documents and a point of contact.