Report Purpose:

Assertion 10

Author:

Admin and Governance Manager

Background

Following the release of Assertion 10, local councils need to have implemented certain regulations to comply, with the AGAR submission 25/26.

The items that need to be in place are as follows:

- Authority owned email address' and website
- An IT policy
- The website must include an accessibility statement
- Website Accessibility Compliance must be WCAG2.2.AA
- A Data protection policy

Below is an extract from the 2025 Practitioners' Guide outlining them all in more depth.

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.

5.124. Data Protection - To ensure compliance with data protection regulations, smaller authorities must:

- *Appoint a Data Protection officer to oversee data protection and ensure compliance with GDPR. (NB NALC has clarified this item with an Addendum as follows 'Under Section 7 of the DPA 2018, Parish Councils and Parish Meetings are exempt from this requirement').*

- *Conduct regular data audits to identify what personal data is held, how it is used and make sure it is processed lawfully.*

- *Implement a Data Protection policy on data handling, storage and sharing.*

- *Provide regular training to ensure all staff and members are trained on data protection principles and practices.*

- *Secure data using appropriate technical and organisational measures to protect personal data from breaches.*

5.125. The Freedom of Information Act places a duty on every public authority to adopt and maintain a publication scheme which details the publication of information by the authority and is approved by the Information Commissioner; adoption of the Information Commissioners Office model publication scheme meets this requirement.

Compliance

Macclesfield Town Council was largely compliant, with the only required update being an amendment to the IT Policy to incorporate Data Protection training. Although the training had already been completed, it was not previously documented in the policy. The updated IT Policy is included on the agenda, and once approved, the Town Council will be fully compliant with Assertion 10.