Assertion 10 Checklist

Council Hive Toolkit
Resource Pack

BREAKTHROUGH COMMUNICATIONS

SPECIALISTS IN CONNECTING COUNCILS WITH THEIR COMMUNITIES

Assertion 10 Check List

ASSERTION 10 CHECKLIST **3**

Copyright and Disclaimer

Understanding and Using This Assertion 10 Checklist

This checklist helps your council assess its compliance with the digital communication, data protection, and transparency expectations ahead of the Annual Governance and Accountability Return (AGAR) for the year 2025/26.

Each item helps you demonstrate accountability, protect information, and build public trust through good governance.

A friendly reminder: data protection compliance is not a one off task - it is a continuous journey.

Good data protection and information compliance require more than just ticking a box once a year. It involves ongoing habits, clear policies, and a commitment to keeping your council's information secure and well-managed.

For the first time, Assertion 10 on the AGAR brings formal attention to how councils handle digital communication and data responsibilities. Whilst this may feel like a new area of focus, in reality most of these duties - from using secure IT systems to maintaining a publication scheme - have long been obligations or best practices under UK General Data Protection Regulations (UK GDPR), the Data Protection Act 2018, and other laws.

We recognise that many councils are already working hard to meet these standards. We also understand that, for a variety of reasons - whether changes to council membership, limited capacity, or uncertainty about requirements - some areas may have become overlooked or delayed.

That is exactly why this checklist exists: not to criticise, but to support. It is here to help you reflect, reset, and take practical steps toward strengthening your digital and information foundations. Even if your council is starting from scratch or catching up, there's no shame in that. What matters most is taking steps in the right direction.

Small improvements can have a big impact, and this checklist will guide you through them.

Assertion 10 Checklist

To sign off this assertion you MUST have taken the following actions. Guidance to help achieve assertions are in *italics*.

Authority-Owned Email Compliance

- ☐ We have an email address on a council owned domain name for general correspondance from the public.

The Practitioners' Guide 2025 states:

"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."

Guidance:

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

Website Accessibility and Legal Compliance

- ☐ The council ensures its website complies with the **Web Content Accessibility Guidelines (WCAG) 2.2 AA**.

- ☐ The council publishes and maintains a clear **accessibility statement**, that outlines any accessibility limitations, how to request alternative formats,

and a named contact for accessibility issues.

- ☐ The council ensures the website complies with the **Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018**, where applicable.

The Practitioners' Guide 2025 states:

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

"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)."

Guidance:

- *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.*

Freedom of Information and Transparency

- ☐ The council adopts and publishes the Information Commissoner's Office (ICO) **Model Publication Scheme**.

- ☐ The council publishes information as required by the:

    - **Transparency Code for Smaller Authorities** (for those with turnover under £25,000)

    - **Local Government Transparency Code 2015** (as best practice for those over £25,000)

- ☐ The council keeps all required financial and governance information is up to date and makes it accessible via the its website.

The Practitioners' Guide 2025 states:

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

Guidance:

- *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 ICO; adoption of the ICO model publication scheme meets this requirement.*
- *In addition to this the Transparency Code for Smaller Authorities requires parish councils with an annual turnover not exceeding £25,000 to publish certain information set out in the code. This enables local electors and local taxpayers to access relevant information about the authority's accounts and governance.*
- *Smaller Authorities with total turnover or expenditure greater than £25,000 should as best practice comply with the Local Government Transparency Code 2015; the government believes that in principle all data held and managed by local authorities should be made available to the public unless there are specific sensitivities to doing so.*
- *Monitoring an authority's compliance with the relevant transparency code is not part of the external auditor's limited assurance review of the AGAR. It would however be expected that internal auditors would review this control area.*

Data Protection and UK GDPR Compliance

- ☐ The council has considered its data protection compliance and is sure that it is fully complying with the UK General Data Protection Regulation (UK GDPR) 2016 and the Data Protection Act (DPA) 2018.

- ☐ The council is processing personal data with care and in line with the principles of data protection.

- ☐ The council has implemented an IT policy that directs how the authority conducts business in a secure and legal way. This policy must cover data when it is processed on both authority equipement and software and personal equipment and software.

The Practitioners' Guide 2025 states:

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

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

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

Guidance:

- *To ensure compliance with data protection regulations, smaller authorities should:*
    - *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*
    - Regularly conduct **data mapping** to identify personal data held and ensure lawful processing.
    - Appropriate **data protection policies** shoudl be in place, that are tailored to the council's operations.
    - Apply technical and organisational **measures to protect personal data** such as secure passwords, encryption, and access controls.
    - Provide **data protection training** to all staff, councillors, and

volunteers.

- **Handle** Subject Access Requests and FOI requests through structured procedures.
- All council members and staff use email accounts hosted on an authority-owned domain (e.g. using `.gov.uk` or `.org.uk`).
- Council members and staff do not conduct business using personal or free webmail services such as Gmail or Outlook.
- The council shoudl mandates the use of authority-owned email accounts for official communications.

Information Technology (IT) Policy

- ☐ The council has implemented an **IT policy**, covering:
  - ☐ Use of council and personal devices for official business
  - ☐ Email, document handling, data storage, and security protocols
  - ☐ Responsibilities of councillors, staff, and contractors
- ☐ The policy provides guidance on cyber security threats such as phishing, and outlines mitigation measures.
- ☐ The council reviews the policy annually and shares it with all relevant parties.

The Practitioners' Guide 2025 states:

"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."

Guidance:

- *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.*
- *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.*