SMALLER AUTHORITIES PROPER PRACTICES PANEL

Suggested Digital Forms to Support AGS Assertion 10 — Digital and Data Compliance

Document Type
Advisory Report

Date
March 2026

Applies To
All Smaller Authorities in England

AGAR Effective From
2025/26 financial year

1. Background and Purpose

Assertion 10 — Digital and Data Compliance is a new assertion introduced in the SAPPP Practitioners' Guide 2025, taking effect from the 2025/26 Annual Governance and Accountability Return (AGAR). It consolidates and expands digital governance requirements previously contained within Assertion 3, bringing together obligations relating to email management, website compliance, GDPR, the Freedom of Information Act 2000, and IT policy.

It is important to note that Assertion 10 does not itself list specific forms that must be created. Rather, it sets out legal and governance requirements that smaller authorities must satisfy. This report identifies the digital forms that would best support a smaller authority in evidencing compliance with those requirements — providing audit trails, enabling statutory processes, and demonstrating proper data governance.

The six forms described in this report are not exhaustive but represent the most impactful areas where digital processes can replace manual or paper-based methods, directly supporting the authority's ability to answer 'Yes' to Assertion 10.

2. Summary of Recommended Digital Forms

The table below provides an at-a-glance overview of the six recommended forms, the specific paragraphs of Assertion 10 they support, and their priority level.

Form Name	Assertion 10 Reference	Priority
Data Subject Access Request (DSAR) Form	Para. 1.51, 1.52, 5.117, 5.120, 5.124	**Essential**
Freedom of Information Request Form	Para. 1.50, 5.120, 5.125, 5.126	**Essential**
Website Accessibility Statement & Feedback Form	Para. 1.48, 1.49, 5.123	**Essential**

Form Name	Assertion 10 Reference	Priority
IT Policy Acknowledgement Form	Para. 1.54, 5.121, 5.122	**Recommended**
Internal Data Breach Reporting Form	Para. 1.51, 1.52, 5.124	**Recommended**
Annual Data Audit Record	Para. 5.124	**Best Practice**

Priority definitions: Essential = directly required to demonstrate compliance; Recommended = strongly supports compliance evidence; Best Practice = aids internal governance and audit trail.

3. Detailed Form Descriptions

Form 1: Data Subject Access Request (DSAR) Form

Assertion 10 Reference	Paragraphs 1.51, 1.52, 5.117, 5.120 and 5.124 of the Practitioners' Guide 2025
Legal Basis	General Data Protection Regulation (GDPR) 2016 and Data Protection Act (DPA) 2018
Priority	Essential

Purpose

All smaller authorities, including parish meetings, must comply with the GDPR and DPA 2018. Under these regulations, any individual whose personal data is held by the authority has the right to request access to that data. Paragraphs 1.51 and 1.52 make clear that all smaller authorities must process personal data in line with the principles of data protection, and paragraph 5.120 specifically notes that authority-owned email accounts make Data Subject Access requests easier to manage.

A dedicated digital DSAR form ensures requests are received, logged, and responded to within the statutory 30-day timeframe. It removes ambiguity about what information is being requested and creates a clear audit trail demonstrating the authority's compliance.

Recommended Fields

Field	Purpose
Full name of requester	Identifies the data subject making the request
Contact email address	For correspondence and delivery of response
Contact telephone number	Optional alternative contact method
Description of data requested	Allows the authority to locate relevant records

Field	Purpose
Date of request (auto-generated)	Starts the statutory 30-day response clock
Proof of identity	File upload field to verify identity before release
Relationship to authority	e.g. resident, employee, member, contractor
Preferred response format	Digital or paper copy preference
Declaration / signature	Confirms the requester's identity and consent

Additional Guidance

The form should be published on the authority's website in an accessible format. A confirmation email should be sent automatically upon submission. The authority's Clerk should be notified immediately, as the 30-day response deadline is statutory. Where an authority has appointed a Data Protection Officer (paragraph 5.124), they should be copied on all submissions.

Form 2: Freedom of Information (FOI) Request Form

Assertion 10 Reference	Paragraphs 1.50, 5.120, 5.125 and 5.126 of the Practitioners' Guide 2025
Legal Basis	Freedom of Information Act 2000 and the Transparency Code for Smaller Authorities
Priority	Essential

Purpose

Paragraph 1.50 requires all authority websites to include published documentation as specified in the Freedom of Information Act 2000. Paragraph 5.125 confirms that every public authority must adopt and maintain a publication scheme, with adoption of the ICO model publication scheme satisfying this requirement. Beyond proactive publication, the FOI Act grants individuals the right to request information not covered by the publication scheme.

A digital FOI request form makes the process straightforward for residents, ensures the authority captures all necessary information to process the request, and provides an automatic record of requests received. This directly supports the authority's transparency obligations and assists internal audit review as referenced in paragraph 5.128.

Recommended Fields

Field	Purpose
Full name of requester	Identifies the person making the request
Email address	Primary contact and method of response

Field	Purpose
Postal address (optional)	Required if hard copy response requested
Description of information requested	Clear description of what information is sought
Date of request (auto-generated)	Starts the 20 working day response period
Preferred format of response	Electronic, printed, or inspection of records
Is this a repeat request?	Helps authority assess whether refusal applies
Submission confirmation	Auto-generated receipt and reference number

Additional Guidance

The authority must respond within 20 working days. If the request is refused (e.g. due to exemptions), the refusal must be issued in writing with the reason stated. The form should link clearly to the authority's publication scheme so requesters can first check whether information is already published. Authorities with turnover above £25,000 should also comply with the Local Government Transparency Code 2015 (paragraph 5.127).

Form 3: Website Accessibility Statement and Feedback Form

Assertion 10 Reference	Paragraphs 1.48, 1.49 and 5.123 of the Practitioners' Guide 2025
Legal Basis	Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018 and WCAG 2.2 AA
Priority	Essential

Purpose

Paragraphs 1.48 and 1.49 state that all smaller authorities (excluding parish meetings) must meet the legal requirements for existing websites and that all websites must meet the Web Content Accessibility Guidelines (WCAG) 2.2 AA standard under the Accessibility Regulations 2018. Paragraph 5.123 further clarifies that at a minimum, all authorities must include an accessibility statement on their website and keep it under regular review.

The accessibility statement must include reasons for any unmet accessibility requirements, ways to obtain alternative copies of non-accessible documents, and a point of contact. A digital feedback form embedded alongside the accessibility statement provides residents with the mechanism to report accessibility issues or request alternative formats, satisfying this contact requirement directly.

Accessibility Statement — Required Content

Field	Purpose
Compliance status	States whether the site is fully, partially, or not compliant with WCAG 2.2 AA
Known accessibility issues	Lists specific known issues and the reason they have not been resolved
Disproportionate burden statement	If applicable, sets out why full compliance would be disproportionate
Alternative format contact	How residents can request accessible versions of documents
Date of last review	Must be kept under regular review
Date of statement preparation	Required field under the Regulations

Feedback Form — Recommended Fields

Field	Purpose
Name of person reporting	For correspondence purposes
Email or telephone	Contact details for response
Description of accessibility issue	Free text description of the barrier encountered
Page or document affected	URL or document name where the issue was found
Alternative format request	Specific format needed, e.g. large print, audio, Braille
Date submitted (auto-generated)	For authority's response tracking

Form 4: IT Policy Acknowledgement Form

Assertion 10 Reference	Paragraphs 1.54, 5.121 and 5.122 of the Practitioners' Guide 2025
Legal Basis	GDPR 2016, DPA 2018, and the authority's own IT policy
Priority	Recommended

Purpose

Paragraph 1.54 requires all smaller authorities (excluding parish meetings) to have an IT policy explaining how clerks, members and other staff should conduct authority business in a secure and legal way when using IT equipment and software, including both authority-owned and personal equipment.

Paragraph 5.122 states that the IT policy prevents misunderstandings when using IT equipment for authority business, and that there can be 'no excuses for anyone in your authority not protecting

their data or working safely.' A digital acknowledgement form ensures that every clerk, member and member of staff has confirmed they have read, understood, and will comply with the policy. This provides a clear audit trail that is essential for demonstrating compliance to internal auditors.

Recommended Fields

Field	Purpose
Full name	Identifies the individual confirming compliance
Role within the authority	e.g. Clerk, RFO, Member, Support Staff
Date IT policy was issued / last updated	Links acknowledgement to the correct policy version
Confirmation of reading	Checkbox: 'I confirm I have read and understood the IT policy'
Confirmation of compliance	Checkbox: 'I agree to comply with this policy'
Understanding of personal device use	Checkbox: 'I understand this policy applies to personal devices used for authority business'
Date signed	Auto-generated or manually entered
Signature (or digital equivalent)	Electronic signature or typed name as declaration

Additional Guidance

This form should be completed by all new clerks and members upon joining, and by all existing staff and members whenever the IT policy is updated. Completed forms should be retained securely for audit purposes. The Clerk should maintain a log of who has completed the form and when. The authority should reissue the form at least annually or following any significant change to the IT policy.

Form 5: Internal Data Breach Reporting Form

Assertion 10 Reference	Paragraphs 1.51, 1.52 and 5.124 of the Practitioners' Guide 2025
Legal Basis	GDPR 2016 Article 33 — Breach notification to supervisory authority within 72 hours
Priority	Recommended

Purpose

Paragraphs 1.51 and 1.52 require all smaller authorities to follow the GDPR and DPA 2018 and to process personal data with care. Paragraph 5.124 requires authorities to implement technical and organisational measures to protect personal data from breaches. A critical element of this is having a clear internal process for reporting suspected data breaches quickly, so the authority can

assess whether a breach must be reported to the Information Commissioner's Office (ICO) within the 72-hour statutory window.

Without a structured reporting form, incidents may go unrecognised or be reported too late. A digital form available to all staff and members ensures that anyone who suspects a breach can report it immediately, regardless of their technical knowledge.

Recommended Fields

Field	Purpose
Name of person reporting	Identifies who discovered the incident
Role within the authority	Clerk, member, contractor, etc.
Date and time incident discovered	Critical for calculating the 72-hour reporting window
Date and time incident occurred (if known)	May differ from discovery date
Description of what happened	Full account of the nature of the breach
Type of data affected	e.g. names, addresses, financial data, sensitive personal data
Estimated number of individuals affected	Helps assess severity
How the breach occurred	e.g. lost device, email sent to wrong recipient, hacking
Immediate action already taken	Steps already taken to contain the breach
Has data left the authority's control?	Yes/No — critical for ICO reporting assessment
Any individuals at risk of harm?	Yes/No/Unknown — informs urgency of response

Additional Guidance

Upon receipt of a completed form, the Clerk (or Data Protection Officer if appointed) must assess within 72 hours whether the breach is notifiable to the ICO. Not all breaches require reporting — only those likely to result in a risk to the rights and freedoms of individuals. The authority should maintain a breach log regardless of whether the breach is reported externally. This log is itself an element of GDPR compliance.

Form 6: Annual Data Audit Record

Assertion 10 Reference	Paragraph 5.124 of the Practitioners' Guide 2025

Legal Basis	GDPR 2016 — Principle of accountability (Article 5(2))

Priority	Best Practice

Purpose

Paragraph 5.124 states that smaller authorities must conduct regular data audits to identify what personal data is held, how it is used, and to make sure it is processed lawfully. An annual data audit record provides the structured framework for conducting this review. It is also directly relevant to the GDPR's accountability principle, which requires authorities to be able to demonstrate their compliance.

Internal auditors reviewing Assertion 10 compliance (as noted in paragraph 5.128) will expect to see evidence that such reviews have been conducted. A completed annual data audit record provides exactly this evidence.

Recommended Fields

Field	Purpose
Data category	e.g. personnel records, member details, financial data, CCTV, hall hire bookings
Type of personal data held	e.g. names, addresses, dates of birth, bank details
Legal basis for processing	e.g. legal obligation, legitimate interests, consent
Where data is stored	e.g. cloud software, local PC, paper files, email system
Who has access	Roles that can access this category of data
Retention period	How long the data is kept before secure deletion
Date of last review	When this data category was last checked
Action required	Any gaps or changes needed to ensure lawful processing
Date action completed	Records when remedial action was taken
Name of person completing audit	Accountability for the review
Date of audit	For version control and annual tracking

Additional Guidance

This record should be completed at least annually, ideally before the financial year end. The completed audit should be reported to members and minuted, demonstrating that the authority has actively reviewed its data handling. The record should be retained securely and made available to internal auditors on request. Where the audit reveals data held without a clear legal basis, appropriate action — including deletion — should be taken promptly and recorded.

4. Implementation Recommendations

Smaller authorities should consider the following approach when implementing these digital forms.

Step 1 — Assess existing provision

Review whether any of these processes currently exist in paper form. Existing paper forms can often be adapted into digital equivalents using the council website, free tools such as Google Forms or Microsoft Forms, or purpose-built council software packages.

Step 2 — Prioritise by compliance risk

The three Essential forms — DSAR, FOI, and Accessibility Feedback — carry statutory deadlines and directly affect the authority's legal obligations. These should be implemented first. The Recommended forms provide evidence of internal governance and should follow as soon as practicable.

Step 3 — Publish and signpost

All public-facing forms (DSAR, FOI, and Accessibility Feedback) must be clearly signposted on the authority's website. They should be easy to find from the homepage and should be accessible in line with WCAG 2.2 AA requirements. Internal forms (IT Policy Acknowledgement, Breach Reporting, and Data Audit) should be made available to all relevant staff and members.

Step 4 — Minute the adoption

The adoption of these forms and any related policies should be recorded in the authority's formal minutes. This provides the documentary evidence required to support a 'Yes' answer to Assertion 10 when the AGAR is completed from 2025/26 onwards.

Step 5 — Review annually

All forms should be reviewed at least annually to ensure they remain fit for purpose and reflect any changes in legislation, guidance, or the authority's own policies. The date of review should be recorded.

5. Conclusion

Assertion 10 represents a significant and welcome formalisation of digital governance requirements for smaller authorities. While the assertion does not mandate specific forms, the six forms described in this report provide practical, proportionate tools that smaller authorities can adopt to demonstrate compliance with the requirements of paragraphs 1.47 to 1.54 of the Practitioners' Guide 2025.

Taken together, these forms support the authority's ability to manage personal data lawfully and transparently, respond to statutory requests within legal timeframes, provide accessible services to residents, and demonstrate to internal auditors that governance processes are in place and operating effectively.

Authorities are encouraged to review their current arrangements against each form described in this report and to prioritise implementation ahead of the 2025/26 AGAR submission, when Assertion 10 will appear on the Annual Governance Statement for the first time.