Demystifying Assertion 10 Compliance & understanding the Practitioners Guide.

Domain Names, Emails, GDPR, Websites & IT Policies

For parish & town clerks and those who administer websites for councils.

What we'll cover

Updates to SAPPP 2025 (formerly JPAG) Practitioners Guide - What the new governance requirement actually means to councils:

- **New Email & domain name requirements** and best practice
- GDPR and data protection responsibilities
- Ensuring **website accessibility compliance** with the **new WCAG2.2AA rules**
- **IT policies and Assertion 10 explained**: – and how it all fits in together – creating the digital and data scope and purpose.

What's it all about?

2025 edition of the *Practitioners' Guide* (Assertion 10: Digital and Data Compliance) *states:*

All smaller authorities, by AGAR 2025/2026, must have:

- A council-owned domain based official email address
- A website that continues to meet accessibility regulations
- An IT policy
- And a reinforcement of compliance with GDPR and DPA responsibilities.

Assertion 10 - Digital and data compliance

WHY? (added to clarify data compliance, previously covered under Assertion 3)

Assertion 10 will appear on the **AGAR 2025-26** By then, 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

Not abcparishclerk**@gmail.com** or abcparishcouncil**@outlook.com**

Councillors & other staff email addresses.

Strangely, Assertion 10 doesn't talk about Councillors and other staff email address compliance – just the clerk/officer.

Best practice is for all council to have matching email:

Cllr.bobsmith@abcparishcouncil.gov.uk

Free email services are permitted currently but NOT personal:

cllrbobsmith@gmail.com **– OK**

BUT NOT bigbobsmith1968@yahoo.co.uk **= GDPR risk/loss of email data/comms**

Why is that important?

- The Council does not own those free platforms or domain (Gmail, Yahoo, Hotmail etc)
- The data contained in it is not really yours
- The Council has no legal rights over it
- Getting access without the logins is impossible
- Creates a GDPR exposures with FOI & SAR issues
- No authenticity of message – anyone can set up a free email address!

(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.

(1.54) All smaller authorities (excl. parish meetings) **must also have an IT policy**.

An I.T Policy explains how everyone - clerks, members and other staff - should conduct authority business in a secure and legal way when using IT equipment and software.

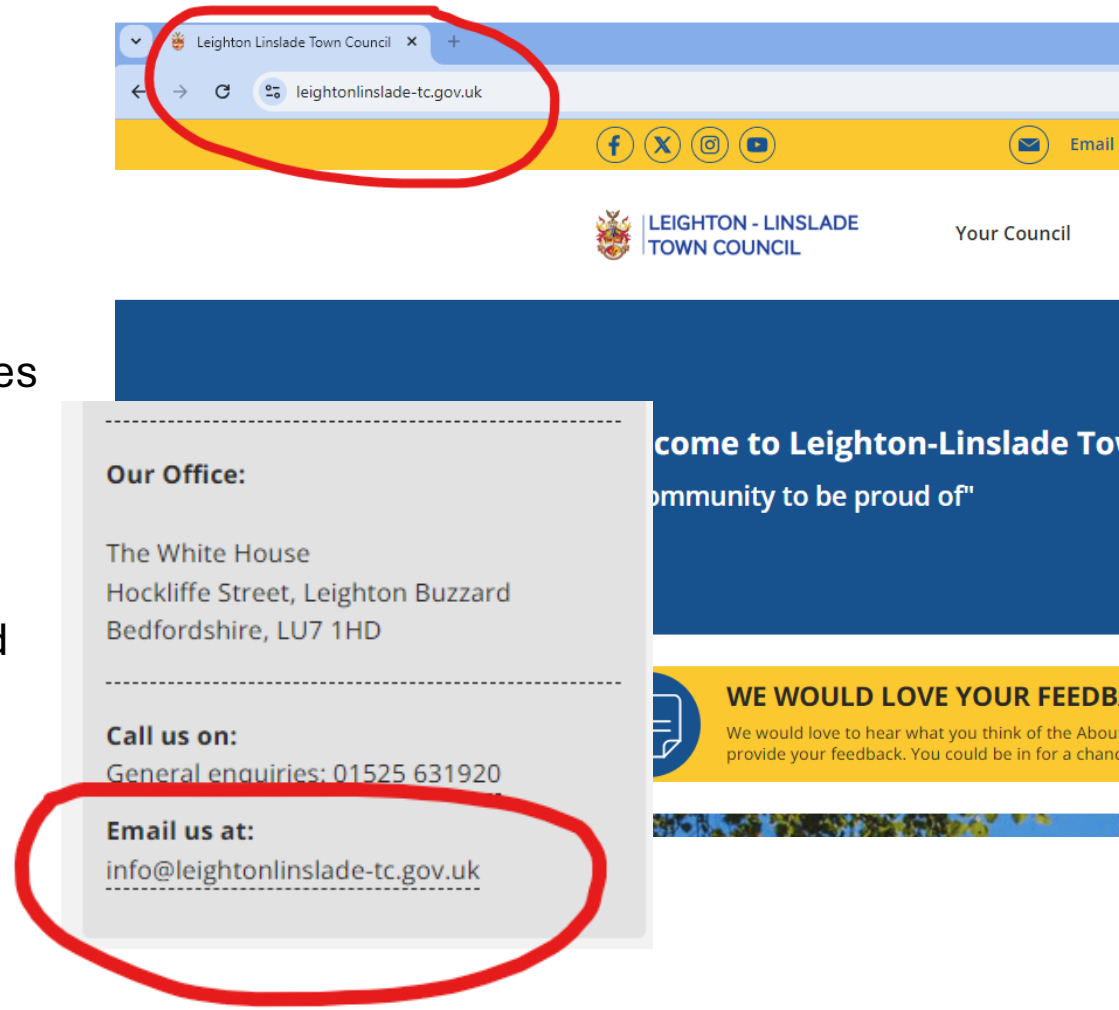
This relates to the use of **authority-owned** and **personal equipment**.

The domain - Your address on the internet

It's **your website address** you use in a web browser, like Google Chrome and Safari for people to see your web pages and information – agendas, minutes, AGAR, news etc

AND

Your email address – the address that people use to send you an email.



.gov.uk

It's the ultimate official domain for a Council.

- Elevated level of security
- Improves compliance
- Improves GDPR – and FOI & SAR situations
- Added benefits and security services
- More professional
- Improved authenticity of message
- Can only be used managed by authorised organisations for added security & governance

.org.uk

It's an acceptable UK-based domain for a Council.

- Elevated level of security above free emails
- Helps with compliance
- Improves GDPR – and FOI & SAR situations
- Requires less scrutiny so = less official than .gov.uk

You *can* also use .com, .co.uk or other council-owned domain suffix but they are not within the UK jurisdiction managed by Nominet.

Aubergine

Best practice

Aubergine offer a .gov.uk domain free for the first year worth £100!

- Claim your parish or town council .gov.uk address
- Use it for matching **email** and **website address.** There are three naming options:

  For parishes**: locationparishcouncil.gov.uk** or **location-pc.gov.uk** or **locationparish.gov.uk**
  For towns: **locationtowncouncil.gov.uk** & **location-tc.gov.uk**
  For community councils: **locationcommunitycouncil.gov.uk** or **location-cc.gov.uk**

- **You CANNOT have abc.gov.uk** – these are reserved for central government.
- Can be used to access .gov.uk GDS central services
- Access to GovPay card payment services on your website
- Improved protection & security with free NSCS Early Warning and filtering services

Domains - recap

- Use a **council-owned domain** for your **website** address
- Use a **council-owned domain** for your official **email** for the council
- Get your **.gov.uk domain for best practice**
- Other council-owned domains are currently acceptable, but website and email should match
- Stop using free email (Gmail/Hotmail/Yahoo etc)
- Consider asking an approved .gov.uk registrar (such as Aubergine) to secure the domain
- Make sure you set enough in the **budget/precept planning for these services**
- Make sure the **domain name is registered to the council** – not an individual.

UK GDPR & DPA continued compliant

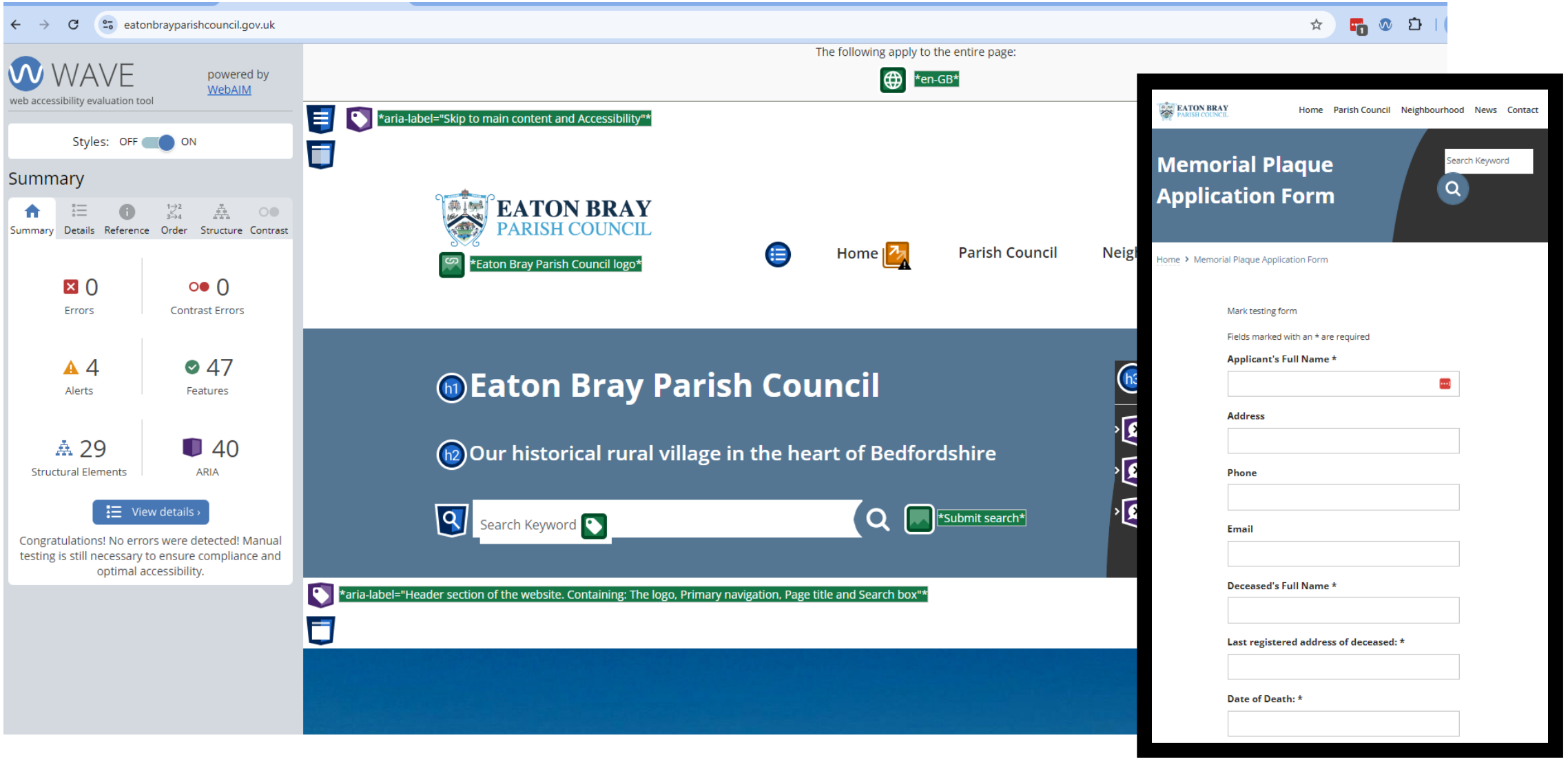
- In short, you need to continue to comply with UK GDPR and DPA – Data Protection Act
- Consider taking a Data Roadmap test
- Use the outcome of that to help define your privacy and other data-related policies, such as data retention.
- Consider asking Data Compliance experts, Breakthrough Communications, for an assessment or guidance.

Website Accessibility Compliance - update

- Regulations for all public sector bodies, incl parish & town councils' websites must meet WCAG2.1AA standard since 2020 **Regulations rose to WCAG2.2AA in October 2024**
- You must have a compliant website
- Regardless of the domain type, SAPPP '25 & Public Sector Website laws require compliance
- You must have an up to date and relevant Accessibility Statement
- Overlays (accessibility plugins) & pop ups risk WCAG2.2AA failure & create barriers
- .gov.uk domains must not be used in a non-compliant way
- Risks? Challenged by vexatious MOP, audit failure, withdrawal of your .gov.uk domain

Website Accessibility tips

- Ensure the website & the content you upload is accessible
- Define your Accessibility Statement and include the things you know are not accessible – 3rd party documents, content older than 2018
- Avoid using 'accessibility plugins' to achieve compliance – they aren't enough
- Have a checking process – use the free browser checker **Wave by WEBAIM** to check as you go
- Make sure any forms are web page forms, not documents
- Consider commissioning an accessibility audit to understand your position
- Consider commissioning a purpose-built website from council website experts, Aubergine, that's .gov.uk-ready and fully compliant from £499 + VAT


eatonbrayparishcouncil.gov.uk
WAVE
web accessibility evaluation tool
powered by WebAIM
Styles: OFF ON
Summary
Summary Details Reference Order Structure Contrast
0 Errors
0 Contrast Errors
4 Alerts
47 Features
29 Structural Elements
40 ARIA
View details ›
Congratulations! No errors were detected! Manual testing is still necessary to ensure compliance and optimal accessibility.
The following apply to the entire page:
en-GB
aria-label="Skip to main content and Accessibility"
EATON BRAY PARISH COUNCIL
Eaton Bray Parish Council logo
Home
Parish Council
Eaton Bray Parish Council
Our historical rural village in the heart of Bedfordshire
Search Keyword
Submit search
aria-label="Header section of the website. Containing: The logo, Primary navigation, Page title and Search box"
EATON BRAY PARISH COUNCIL
Home Parish Council Neighbourhood News Contact
Memorial Plaque Application Form
Search Keyword
Home › Memorial Plaque Application Form
Mark testing form
Fields marked with an * are required
Applicant's Full Name *
Address
Phone
Email
Deceased's Full Name *
Last registered address of deceased: *
Date of Death: *

Website Accessibility tips

- Avoid using tables where possible
- Add ALT text for images
- Avoid embedding text on images
  – events need the salient info on the web page
- High Contrast
- Use sequential headings
- Make documents accessible before uploading
- Forms need to be web forms, not PDFs
- Use descriptive link text (not ‘click here’!)
- Avoid pasting URLs on the page
- Avoid overly styled text formatting
- Avoid ‘accessibility plugins’
- Avoid scans where possible
  (3rd party documents/AGAR/ROI excluded)
- Have a regular checking process
- Revisit your accessibility statement

Website Accessibility tips

- **Budget for it – precept planning is ahead**
- **Share accessibility publishing goals with colleagues**
- **Ahead of AGAR25/26 have an action plan – your auditors will**
- **It’s not just the law, it’s the right thing to do!**

Question time

What is an IT policy?

A formal IT policy provides a simple, central document outlining how the Council's digital tools and information should be used and how they are managed securely and professionally.

The policy 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**.

Aren’t there templates?

Sort of.

A policy of this kind reflects the council’s OWN practices and what Council wants to define in the scope.

Templates will have certain things to consider as a minimum such as email & usage/online behaviour/what the council does in an emergency (data breach) and other protocols

There is no ‘boiler plate’ to copy verbatim.

Why?

- As local authorities shift more of their operations online—emailing agendas, sharing sensitive documents, updating websites, and even engaging on social media—having clear digital protocols has become essential.
- Councils store and use people's data
- Without proper guidance, authorities risk being exposed from the following possibilities…

Areas of risk include:

- **Data leaks** from unsecured platforms (email, websites, shared files) or mishandled personal information.
- **Lost communications** when staff or councillors use personal accounts that are inaccessible when they leave (Gmail, Hotmail etc not owned by the Council).
- **Regulatory failures**, such as non-compliance with accessibility laws or mishandling Freedom of Information (FOI) requests.
- **Cybersecurity threats** including phishing, malware, or compromised devices & email accounts.

What goes in a good IT policy:

- **Scope and purpose**
- **Official email protocol**
- **Data protection, storage and GDPR compliance**
- **Data retention**
- **Website standards & accessibility (WCAG 2.2)**
- **Cybersecurity basics**
- **Social media use and boundaries**

Common pitfalls to avoid

- Common Pitfalls to Avoid
- Too technical or redundant (link to other policies instead)
- Unworkable rules without proper tools
- Allowing personal accounts for council work
- Skipping exit procedures (hardware, access, passwords)
- Failing to assign responsibility or consult experts
- Don’t copy policies blindly – tailor to your council’s needs

Key Elements of an Effective Council IT Policy

- Key Elements of an Effective Council IT Policy
- Use of Council Devices
- Only for Council business; no unauthorised software
- Return equipment and revoke access when leaving role
- Clear support and issue-reporting process
- Cybersecurity Best Practices
- Use anti-virus, 2FA, and strong, unique passwords
- Train staff to spot phishing and suspicious links
- No password reuse across accounts
- Training & Review
- Annual training on IT use & data protection
- Assign policy review responsibility; review yearly
- Data Breaches & Risk Management
- Define clear breach response steps & timelines
- Identify where personal data is stored/accessed
- Regularly assess risk points (e.g., emails, devices, cloud)

What to do next:

If you don't already have an IT policy in place:

- Use a template from your County Association, SLCC, or NALC **as a starting point**.
- Customise it to reflect **your specific council setup** and digital tools & processes.
- **Adopt the policy** formally at a council meeting and record the decision in the minutes.
- **Ensure training so all members** understand their roles and responsibilities.
- **Annually review the policy** – has anything changed (process or equipment) since the last review?

Final Word

- This is more than a paperwork exercise.
- A well-considered IT policy protects your council's data, maintains legal compliance, and supports good digital governance.
- It wraps around the counterpart digital aspects – accessibility compliance, use of .gov.uk domains and official email addresses and best practice and more professional methods of operating.
- Now that it's a formal part of the SAPPP Practitioners' Guide, it's not optional—it's essential.
- If you're unsure how to proceed, your internal auditor or your Association is a good place to begin.
- Better to be proactive now than face challenges down the line.