Assertion 10 – Digital and Data Governance Compliance Checklist

Assertion 10 of the Annual Governance and Accountability Return (AGAR) is a new requirement for English local councils, effective from the 2025/26 financial year, that formalizes digital and data compliance. It requires councils to have an IT policy, use a council-owned domain for official email, ensure their website meets WCAG 2.2 AA accessibility standards, and comply with data protection legislation like the UK GDPR. This replaces previous, implied requirements under Assertion 3 to give digital governance and data protection requirements their own standalone section

1. Email and Communication Systems

- All official correspondence uses a Council domain email address (e.g., @highcliffewalkford-pc.gov.uk).
- Email systems are monitored, backed up, and secured with appropriate IT controls.
- Email policies exist and are regularly reviewed.
- Councillors' official communications follow GDPR principles and Council communication policy.

---

2. Website Accessibility and Information

- The Council's website complies with **Web Content Accessibility Guidelines (WCAG) 2.2 AA** standards.
- An up-to-date Accessibility Statement is published on the website.
- Website content is reviewed for accessibility compliance (alt text for images, correct document formats, appropriate colour contrast, etc.).
- Website content is kept up to date, including agendas, minutes, policies, and financial information as required by the Transparency Code.
- Publication of Council information aligns with the ICO Model Publication Scheme.

---

3. Data Protection Compliance (UK GDPR & DPA 2018)

- A Data Protection Policy is adopted and reviewed annually.
- A Data Protection Officer or designated responsible officer is appointed.
- A record of processing activities is maintained.

- Data Protection Impact Assessments (DPIAs) are conducted for relevant projects.
- Procedures exist for Subject Access Requests (SARs) and are compliant with statutory timelines.
- Secure storage and disposal protocols for personal data are in place.

---

4. Freedom of Information (FOI) Compliance

- An FOI Policy is adopted and publicly available.
- The Council has adopted the ICO Model Publication Scheme.
- A clear procedure exists for handling FOI requests.
- The Council responds to FOI requests within statutory deadlines (20 working days for FOI, 40 working days for EIR where applicable).
- A Disclosure Log is maintained and accessible on the website.

---

5. IT and Cybersecurity Governance

- IT policies and acceptable use guidelines are in place for councillors, staff, and volunteers.
- Antivirus, firewall, and software update protocols are in place and regularly reviewed.
- Backups of digital records are performed regularly and securely stored.
- Cybersecurity training is provided to all relevant parties.

---

6. Record-Keeping and Audit Trail

- All key decisions, agendas, and minutes are published in line with Transparency Code requirements.
- A document retention policy is adopted and implemented.
- Records of FOI, SAR, and other information governance requests are maintained.
- An internal audit trail exists to confirm compliance with data protection and FOI obligations.

---

7. Training and Awareness

- All councillors and staff receive regular training on FOI, GDPR, and website accessibility obligations.
- Training records are maintained.

---

8. Annual Review

- A formal review of Assertion 10 compliance is conducted annually before approving the AGAR.
- Any issues identified are addressed and recorded.

Final sign-off:

- Responsible Officer: _____
- Date: _____
- Reviewed by Council: _____