Assertion 10: Digital and Data Compliance

Please note any recommendation within the report are listed again at the end for ease.

The 2025 Practitioners' Guide introduces a new governance requirement — Assertion 10. From 2025–26 onwards, councils must confirm they have taken proper steps to ensure digital and data compliance, including:

- Using a council-owned domain (e.g. clerk@broadstone-tc.gov.uk) rather than personal Gmail/Outlook accounts. Noting org.uk is also acceptable.
  - BTC – Already compliant

- Ensuring websites are compliant with Accessibility Regulations 2018 (WCAG 2.2 AA).
  - BTC – Already compliant

- Publishing required documents under the Freedom of Information Act 2000 and Transparency Code.
  - BTC – Have published everything we have so, far but there are still documents which need to be created, approved and then published.

- Adopting an IT policy covering both council-owned and personal devices.
  - A new policy is being developed.

- Complying with GDPR (2016) and Data Protection Act 2018 for all personal data.
  - BTC already process data in line with the seven principles of data protection.
  - Data mapping is being carried out.
  - Information Commissioners Office (ICO) registration is being processed
  - The Clerk is nominated as the Data Processor and Data Controller.
  - A Data Risk Assessment has been developed and is presented below to Council for discussion and approval.

Risk Assessment: Devices for Councillors

A key decision for the council will be whether to:

1. Provide a device to each councillor (e.g. phone/laptop/tablet pre-configured with council email and security settings).
2. Permit Bring Your Own Device (BYOD), allowing councillors to access gov.uk emails from their own personal devices.

Option 1: Council-Supplied Devices

Benefits

- Stronger control over security, updates, and software.
- Easier compliance with GDPR/DPA 2018.
- Clear separation between council business and private use.
- Simplifies withdrawal of access when a councillor leaves office.

Risks / Costs

- Upfront financial cost of buying and maintaining devices.
- Ongoing IT support and replacement cycles.
- Devices may be under-utilised if councillors only use them occasionally.

Option 2: Bring Your Own Device (BYOD)

The ICO guidance highlights several risks:

- Reduced control: Devices are owned and maintained by individuals, not the council.
- Data leakage: Risk of council data mixing with personal use (e.g. family members using the same device).
- Storage risks: Data may end up on personal cloud backups or removable storage.
- Loss/theft: Personal devices may not have strong security features (e.g. encryption, remote wipe).
- Monitoring issues: Councils may struggle to enforce security without excessive monitoring of private use.

Benefits

- Cost savings — no need to purchase new devices.
- Convenience for councillors already comfortable with their own devices.
- Flexibility — multiple access points.

Risk Mitigation if BYOD is chosen (per ICO guidance):

- Have a clear BYOD policy, including acceptable use, data separation, encryption, and remote-wipe arrangements.
- Limit which personal data can be processed on personal devices.
- Require strong passwords, automatic locking, and regular updates.
- Ensure councillors know what happens to council data if they leave office.

Recommendation

The council should discuss and consider the risk assessment above before deciding whether to provide council-owned devices or allow BYOD.

Key considerations include:

- **Data sensitivity**: Are councillors regularly handling personal data (e.g. residents' complaints, planning applications)?
- **Cost vs. compliance**: Is the expense of supplying devices outweighed by reduced compliance risks?
- **Capacity**: Can the clerk or an IT provider support device management?

In governance terms, providing council-owned devices is the lower-risk option for compliance with Assertion 10. If BYOD is allowed, the council must adopt a robust BYOD policy aligned with ICO guidance to demonstrate risk mitigation.

Risk Assessment Matrix – Assertion 10 (Digital & Data Compliance) Option 1: Council-Supplied Devices

Risk	Likelihood (1–5)	Impact (1–5)	Risk Rating	Mitigation
Upfront and ongoing costs strain budget	4	3	**12 (Medium)**	Budget planning, phased rollout, seek grants.
Devices underused by councillors	3	2	**6 (Low)**	Provide lightweight/low-cost tablets, review usage annually.
Technical support demands on Clerk	3	3	**9 (Medium)**	Outsource IT support or use simple managed devices.
Data breach from lost/stolen council device	2	4	**8 (Low/Medium)**	Encryption, remote wipe, password/PIN protection.

Overall assessment: Lower compliance risk, higher financial cost.

Option 2: Bring Your Own Device (BYOD)

Risk	Likelihood (1–5)	Impact (1–5)	Risk Rating	Mitigation
Loss/theft of personal device exposing council emails/data	4	4	16 (High)	Require encryption, PINs, and remote wipe registration.
Data leakage to personal/family users	3	4	12 (Medium/High)	Sandbox council data (separate apps), councillor training.
Insecure cloud backup of council data	3	4	12 (Medium/High)	Prohibit syncing council data to personal cloud storage.
Councillor leaves office with council data still on device	3	4	12 (Medium/High)	Clear exit process: mandatory data deletion, revoke access.
Inconsistent security updates across many devices	4	3	12 (Medium/High)	Require minimum standards (e.g. supported OS, regular updates).
Difficulty monitoring compliance without intruding on personal privacy	3	4	12 (Medium/High)	Adopt a clear BYOD policy, proportional monitoring only.

Overall assessment: Higher compliance risks, lower financial cost.

Summary Table

Option	Cost Risk	Compliance/Data Risk	Governance Burden	Overall Risk Profile
Council Supplied Devices	High	Low	Medium (support)	Safer for compliance, more expensive
BYOD	Low	High	High (policy enforcement)	Cheaper, but significantly higher compliance risk

Recommendation – Assertion 10 (Digital & Data Compliance)

In light of the new obligations introduced under Assertion 10 of the 2025 Practitioners' Guide, Broadstone Town Council should note current compliance.

Evidence of Current Position

- Using a council-owned domain (e.g. clerk@broadstone-tc.gov.uk rather than Gmail/Outlook). *Noting that .org.uk is also acceptable.*
    - BTC – Already compliant.
- Ensuring websites are compliant with Accessibility Regulations 2018 (WCAG 2.2 AA).
    - BTC – Already compliant
- Publishing required documents under the Freedom of Information Act 2000 and Transparency Code.
    - BTC – Have published everything we have so, far but there are still documents which need to be created, approved and then published.
- Adopting an IT policy covering both council-owned and personal devices.
    - A new policy is being developed.
- Complying with GDPR (2016) and Data Protection Act 2018 for all personal data.
    - BTC already process data in line with the seven principles of data protection.
    - Data mapping is being carried out.
    - Information Commissioners Office (ICO) registration is being processed
    - The Clerk is nominated as the Data Processor and Data Controller.
    - A Data Risk Assessment has been developed and is presented below to Council for discussion and approval.

Recommendations for Discussion and Approval

1. Secure Access: All councillors and officers should access council emails and documents only through secure, council-approved systems.
2. Risk Acknowledgement: The Council should formally note the risk assessment, recognising that while BYOD offers lower financial cost, it introduces significantly higher compliance and data protection risks.
3. Preferred Approach: Subject to available budget, the Council should consider adopting a policy of supplying each councillor with a council-owned device configured to meet digital compliance requirements, or
4. BYOD Policy (if required): If BYOD use is to be permitted, it must be supported by a formal BYOD policy (aligned with ICO guidance) covering security, acceptable use, and councillor responsibilities, for approval by Council before implementation.

Draft Bring Your Own Device (BYOD) Policy – Outline

(For discussion if necessary)

1. Purpose
To set out conditions under which councillors may use personal devices (laptops, tablets, smartphones) to access Council information, while ensuring compliance with GDPR (2016), DPA 2018, and the requirements of Assertion 10.

2. Scope
Applies to all councillors and officers who access council email (.gov.uk domain) or documents using a personal device.

3. Security Requirements
- All devices must:
  - Be secured with a strong password/PIN and auto-lock after inactivity.
  - Use encryption where available.
  - Be kept updated with operating system and security patches.
- Council data must be accessed only through approved applications (e.g. council email app or secure portal).
- Use of removable media (USBs, SD cards) for council data is prohibited unless encrypted.

4. Data Protection
- Council data must not be backed up to personal cloud accounts or shared with third-party apps.
- Personal and council data must be kept separate (e.g. using distinct apps).
- Councillors must only use council data for council business.

5. Loss, Theft, or Leaving Office
- Any loss or theft of a device must be reported immediately to the Clerk.
- Devices must allow for remote wipe or manual deletion of council data.
- On leaving office, councillors must ensure all council data is securely deleted and access revoked.

6. Monitoring and Compliance
- The Council may require confirmation that devices meet these security standards.
- No monitoring of personal use will be carried out beyond ensuring council data is protected.

7. Responsibilities
- Councillors remain personally responsible for protecting council data on their device.
- Breaches of this policy may result in withdrawal of BYOD permission.