Bring your own device – Adopted September 2025

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.