Bring Your Own Device (BYOD) Policy – Councillors

Approved by: Durrington Town Council
Review Date:
Next Review:

1. Purpose

This policy sets out the requirements for councillors using their own devices (laptops, tablets, smartphones) to access council information, emails, or personal data, ensuring compliance with GDPR and UK data protection law.

---

2. Scope

Applies to all councillors who use personal devices for:

- Accessing council email
- Storing, viewing, or editing council documents
- Processing personal data of residents, staff, or councillors

---

3. General Principles

- Personal devices must be **secured with a password or PIN**.
- Devices should have **up-to-date antivirus/anti-malware software**.
- All council documents containing personal data must be stored in **approved encrypted storage** (Council email, cloud storage, or secure device encryption).
- Councillors must **not store sensitive or special category data permanently** on personal devices. Temporary access is allowed only for council business.
- Councillors must **log out** from council accounts after use and **lock devices** when unattended.
- Lost, stolen, or compromised devices must be reported **immediately to the Clerk**.

---

4. Email and Document Access

- Council emails must be accessed using the **official council email account**.

- When sending emails to multiple recipients, **use BCC** to protect personal data.
- Council documents downloaded to personal devices **must be deleted immediately after use**.

---

5. Security Requirements

Councillors using personal devices for council business must ensure that:

- Screen lock is enabled using a password, PIN, or biometric authentication.
- Council data is stored only on encrypted devices or within approved cloud services.
- Operating systems and applications are kept up to date using automatic updates where possible.
- Only approved applications and services are used to **access, store, or transmit council data**, and no software or apps are used that could compromise the security of council information.

---

6. Prohibited Actions

- Sharing council data with unauthorised persons.
- Using personal devices to process council data for non-council purposes.
- Storing personal data on cloud services that are **not council-approved or GDPR-compliant**.

---

7. Monitoring and Compliance

- The Clerk and council officers may request confirmation that councillors comply with this policy.
- Non-compliance may lead to **restricted access to council data**.
- Councillors remain responsible for GDPR compliance when using personal devices.

---

8. Incident Reporting

- Any suspected breach, loss, or unauthorised access of council data **must be reported immediately** to the Clerk.

- The Clerk will manage breaches in line with the council's **Data Breach Policy**.

---

9. Review - This policy will be reviewed **annually** or sooner if regulations or technology change.