PORLOCK PARISH COUNCIL
BRING YOUR OWN DEVICE POLICY

1. Introduction
Porlock Parish Council 'the council' recognises that members and employees may use personally owned devices (e.g. smartphones, tablets, laptops) to conduct Parish Council business. This policy ensures compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

2. Scope
This policy applies to all elected and co-opted members, the Clerk, and all employees or volunteers who access or process council data using personal devices.

3. Responsibilities
All users of personal devices for council business must:

- Ensure devices are secured with strong passwords or biometric authentication,
- Keep devices updated with the latest security patches and antivirus software,
- Use encrypted connections (e.g. VPN or secure Wi-Fi) when accessing council data,
- Avoid using public Wi-Fi unless protected by a secure connection,
- Immediately report any loss, theft, or suspected breach to the Clerk.

4. Data Protection Requirements
- Personal data must only be accessed or processed for legitimate council purposes.
- Data must be deleted from personal devices once no longer required or upon leaving the council.
- Sensitive personal data (e.g. health, political views) must be handled with extra care and only stored on secure systems.
- Council data must not be shared with unauthorised individuals or stored in insecure apps or cloud services.

5. Security Measures
- Devices must auto-lock after a short period of inactivity.
- Council email accounts must be accessed via secure apps or web portals.
- No council data should be stored permanently on personal devices.
- Remote wipe capabilities should be enabled where possible.

6. Monitoring and Compliance
- The council reserves the right to restrict access to council systems from any device that does not meet security standards.
- Users must cooperate with audits or investigations related to data protection.
- Breaches of this policy may result in disciplinary action or referral to the Information Commissioner's Office (ICO).

7. Leaving the Council
Upon leaving the council, members and employees must:

- Permanently delete all council-related data from personal devices and email accounts,
- Return any council-issued equipment,
- Confirm in writing that all data has been removed.

8. Review and Updates
This policy will be reviewed annually or in response to changes in legislation or council operations.

Dated: 10th September 2025

---	---
Duncan McCanlis	Johnathan Jones
Chair	Clerk & Responsible Financial Officer