### A black and white drawing of a building with a tower Description automatically generated with low confidence

**Market Drayton Town Council**

**Bring Your Own Device Policy (BYOD)**

**1. Introduction**

This BYOD Policy outlines the responsibilities and acceptable use of personal devices by employees, contractors, and elected members of the council. It is designed to ensure compliance with the 2025 Practitioners’ Guide, specifically Assertion 10, and to protect the integrity and confidentiality of council data.

**2. Scope**

This policy applies to all personnel who access council data or systems using personal devices, including smartphones, tablets, and laptops.

**3. Policy Objectives**

- Ensure compliance with UK GDPR, Data Protection Act, and Freedom of Information Act.  
- Protect council data accessed or stored on personal devices.  
- Define acceptable use and security requirements for BYOD.

**4. Microsoft 365 Licensing Requirements**

To support BYOD securely, the council must implement the following Microsoft 365 features:

- Microsoft Intune for Mobile Device Management (MDM) and App Protection.  
- Azure AD Premium P1 for Conditional Access and Identity Protection.  
- Microsoft Purview Information Protection for data classification and encryption.  
- Exchange Online Protection and Data Loss Prevention (DLP).  
- Recommended licensing tier: Microsoft 365 Business Premium or higher (E3/E5 for

advanced compliance).

**5. Acceptable Use**

- Personal devices must be registered with Microsoft Intune.  
- Devices must comply with council security policies (e.g., PIN, encryption).  
- Users must not store council data in unapproved apps or services.  
- Council email must be accessed only via approved Microsoft 365 apps.

**6. Security and Compliance**

- Devices must be protected with up-to-date antivirus and OS patches.  
- Council reserves the right to remotely wipe corporate data from personal devices.  
- Users must report lost or stolen devices immediately.  
- Regular audits will be conducted to ensure compliance.

**7. Training and Awareness**

All users must complete mandatory data protection and BYOD training before accessing council systems on personal devices.

**8. Enforcement**

Non-compliance with this policy may result in revocation of BYOD privileges.

**9. Approval and Review**

This policy is approved by the council’s Finance and General Purposes Committee and will be reviewed annually or as required by changes in legislation or technology.