

Ditton Priors Parish Council

Interim IT & Digital Compliance Policy

1. Purpose and Scope

This policy ensures that Ditton Priors Parish Council meets its obligations under **Assertion 10** of the AGAR. It applies to all staff and councillors. As the Council does not provide hardware, this policy governs the use of personal devices for Council business.

2. Official Communications & Domains

- **Official Email:** All Council business must be conducted using the official @dittonpriorsparishcouncil.co.uk email addresses.
- **Prohibition:** The use of personal email addresses (e.g., Gmail, Hotmail, BT) for Council business is strictly prohibited to ensure transparency and FOI compliance.
- **Separation of Data:** Council emails must be kept separate from personal emails within the mail application.

3. Personal Device Security (BYOD)

Where the Clerk or Councillors use personal equipment (Laptops, Tablets, Phones), the following security standards are mandatory:

- **Access Control:** Devices must be password, PIN, or biometric protected.
- **Software Updates:** Operating systems and security software must be kept up to date to protect against vulnerabilities.
- **Encryption:** Council-related documents stored locally on a personal hard drive should be kept in an encrypted folder or a secure cloud environment (e.g., OneDrive/SharePoint) associated with the [.gov.uk](https://www.gov.uk) account.
- **Public Wi-Fi:** Council business involving personal data must not be conducted over unsecured public Wi-Fi without a VPN.

4. Data Protection & Storage

- **Data Controller:** The Council is the Data Controller. The Clerk, as the Data Processor, must ensure no Council data is accessible to other members of their household.
- **Retention:** Data must be stored in accordance with the Council's *Document Retention Policy*.
- **End of Term/Employment:** Upon leaving the Council, the individual must ensure all Council-owned data is transferred to the Council and then securely deleted from their personal device.

5. Website Accessibility

- The Council's website shall be maintained to meet **WCAG 2.2 AA** standards.

- The Clerk will ensure an updated *Accessibility Statement* is published annually, noting any disproportionate burden claims if applicable.

6. Breach Reporting

Any loss of a device containing Council data, or any suspected unauthorized access to Council email accounts, must be reported to the Council (and the appointed Data Protection Lead) within 24 hours to comply with UK GDPR reporting windows.

Updated April 26

Review July 26