WHIMPLE PARISH COUNCIL
BRING YOUR OWN DEVICE (BYOD) POLICY

(*Approved 19 January 2026*)

1. Introduction

Whimple Parish Council 'the council' recognises that councillors and employees may use personally owned devices (e.g. computers [desktop and laptop], smartphones, tablets and external hard drives) to conduct Parish Council business.

The purpose of this policy is to ensure so far as possible that personally owned devices used by councillors and the Parish Clerk to conduct Parish Council business are used in a manner which protects Personal Data and ensures compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

This policy has been written to minimise the risks associated with BYOD by outlining the responsibility and acceptable use.

2. Scope

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

Breach of this policy may result in disciplinary action (employees) or referral to the Monitoring Officer (councillors).

3. Risks

Under normal circumstances the only device holding personal data is the Parish Clerk's computer: provided that the access and safe usage measures are practiced, then no further action is required.

However, should this computer be unavailable for whatever reason, then the Chairperson or other designated councillor may need to use a personal device to conduct parish business: in which case it must be presumed that personal data may be handled.

Before a personal device is used, the Council must be satisfied that all the following safety measures are in place. Once the official laptop is again available, all council data accumulated on the personal device must be deleted.

The Parish Council has identified a number of risks inherent in using personally owned Devices to conduct Parish Council Business which have been added to the Council's Risk Assessment.

4. Responsibilities

All users of personal devices for council business are responsible for protecting the device. This includes regular updating of software and ensuring it is not used by anyone else to gain access to Council information.

The remaining sections of this Policy set out the guidance that individuals must follow when using a personal device for council business.

- 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,
- Ensure that the device is not used by anyone else
- Immediately report any loss, theft, or suspected breach to the Clerk.

5. Access to Devices

- Devices used for Parish Council business must be secured with strong passwords or biometric authentication
- Passwords must comply with the following rules:
    - Passwords must not be written down
    - Passwords must not be disclosed to any other person. If a password is disclosed to any other person, whether deliberately or inadvertently, it must be changed immediately
    - A different password should be used for each and all Devices, email accounts or other hosted systems
    - Passwords should be changed at least every 12 months
    - Passwords should be a complex mix of letters and symbols, at least 8 characters long
- Ensure that the device is not used by anyone else
- You are responsible for paying any network charges that might occur whilst using your device for council business unless otherwise agreed by the Council

6. 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.

7. Safe usage of Devices

- 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

8. 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 (unless there is a robust Data Sharing Agreement in place).

9. **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).

10. **Lost or Stolen Devices**
    In the event that a Device is lost or stolen, or is suspected of having been stolen, the Parish Clerk or Chair and/or Vice Chair (in the event of it being the Parish Clerk's device) must be informed. The Parish Council will work with the owner of the lost or stolen device to identify any personal data at risk and will then take appropriate action, including reporting any breach to the ICO as necessary.

11. **Repair of Devices**
    If a personal device needs to be repaired, the owner will take all reasonable steps to ensure that the repairer cannot access any personal data.

12. **Transfer or Disposal of Devices used for Council Business**
    If the owner wishes to transfer or dispose of a personal device which has been used for Parish Council business all personal data must be deleted from that device using a method which prevents recovery.

13. **Leaving the Council**
    Upon leaving the council, councillors 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.

14. **Review and Updates**
    This policy will be reviewed every two years or in response to changes in legislation or council operations.