Melchbourne & Yelden Parish Council

Bring Your Own Device (BYOD) Policy

1. Introduction

1.1 This policy sets out how personal devices (laptops, tablets, mobile phones) may be used to access Melchbourne & Yelden parish council information, including email and documents.

1.2 Its purpose is to ensure that council information remains secure even when accessed on personal equipment, while keeping requirements proportionate for councillors and the clerk.

2. Device Owner Responsibilities

2.1 Users should take reasonable steps to keep their device secure when accessing council information. This includes:

(a) using a password, PIN or biometric lock

(b) ensuring the device is generally kept up to date and security updates are applied when the device prompts the user

(c) using built-in security tools such as automatic screen lock

(d) keeping devices safe from loss or theft

(e) reporting any loss, theft or suspected unauthorised access to the clerk as soon as possible

2.2 If available, users are encouraged – but not required – to enable remote-wipe capability in case a device is lost.

3. Personal Data and Confidentiality

3.1 Users must ensure that:

(a) council information is accessible only to the authorised councillor or clerk

(b) take reasonable steps to ensure family members or others sharing the device cannot view or retrieve council data

(c) emails and documents containing council information are deleted once no longer required

(d) council data is not forwarded to anyone other than the authorised councillor or clerk

3.2 Personal Data belonging to residents, staff or suppliers must not be stored or shared in personal messaging apps such as WhatsApp, iMessage or Facebook Messenger where this risks accidental disclosure.

4. General Requirements

4.1 Personal devices used for council business may be subject to disclosure in legal proceedings

4.2 Before disposing of a device, all council data must be securely erased

4.3 All council information must be removed from the device when a councillor leaves office or an employee leaves the council

5. Data Protection and GDPR Compliance

5.1 Users must comply with the Data Protection Act 2018 and UK GDPR. This includes ensuring that any personal data relating to residents, councillors, staff or suppliers is handled securely.

5.2 A breach caused by improper use of a personal device may lead to action by the Information Commissioner's Office (ICO) and could result in standards or disciplinary procedures.

6. Technical Requirements

6.1 Users must take reasonable steps to keep their device secure when accessing council information. This includes:

(a) use strong, unique passwords following NCSC guidance (three random words)

(b) use multi-factor authentication (MFA) where supported

(c) avoid unsecured public Wi-Fi when accessing council information

(d) password-protect any confidential documents shared by email

(e) avoid saving council documents directly onto personal cloud accounts

6.2 Where possible, users should maintain a clear separation between personal and council data.

7. Prohibited Actions

7.1 Users must not:

(a) allow any other person to access council information on their device

(b) use their council email address for personal registrations (shopping, social media, private business)

(c) store sensitive council information in unsecure apps

8. Incident Reporting

8.1 Any loss of a device, suspected breach, unauthorised access or suspicious activity must be reported immediately to the clerk.

9. Compliance

9.1 Failure to follow this policy may result in restricted access to council information systems or further action where necessary.

10. Review

10.1 This policy will be reviewed every two years or sooner if legislation changes.

11. Version Control

Version Control Record

Ref.	Date of Update	Details of Amendments/Changes
1	Mar 2026	Initial adoption of policy.