

Melchbourne & Yelden Parish Council

IT & Email Policy

1. Introduction

- 1.1 Melchbourne & Yelden parish council recognises the importance of effective, secure and reliable information technology (IT) to support its activity and communications. This policy provides clear guidance on the appropriate use of email accounts, information, and IT systems by councillors, the clerk and any authorised users.

2. Scope

- 2.1 This policy applies to Melchbourne & Yelden parish councillors and the Clerk.

3. Device and software use

- 3.1 The council has issued the Clerk with a dedicated laptop; no other IT hardware has been issued. Councillors access council information using their own devices.
- 3.2 Users must ensure that personal laptops, tablets and phones used for council purposes are secure, up to date, and protected by strong passwords or biometrics.
- 3.3 Unauthorised software must not be installed on any device used for council work.
- 3.4 Users of personal devices must also comply with the Council's Bring Your Own Device (BYOD) Policy.

4. Data management and security

- 4.1 All council data must be stored securely. Confidential or sensitive material must not be saved to unapproved cloud services or shared accounts. The current approved cloud service is Dropbox.
- 4.2 Documents must be retained only for as long as needed. Secure deletion is required when data is no longer required.

5. Network and internet usage

- 5.1 Internet access when handling council business must be used responsibly. Users must not download or share copyrighted material without permission.

6. Email communication

- 6.1 The Clerk is issued a @melchyeld-pc.gov.uk email address for all council business.
- 6.2 Councillors use their own personal email addresses for council business. Where personal email addresses are used, emails must be professional and respectful
- 6.3 Council business must be kept separate from personal correspondence where possible.
- 6.4 A consistent email address should be used for council matters.
- 6.5 Users must be alert to phishing, spam and suspicious attachments

7. Password and account security

- 7.1 Users must keep passwords secure and never share them.
- 7.2 It is encouraged that passwords follow National Cyber Security Centre (NCSC) guidance (three random words).

- 7.3 Multi-factor authentication should be used where available.
- 7.4 Passwords must be changed immediately if compromise is suspected.
- 7.5 Users must ensure that screens cannot be overlooked when working in public spaces and that documents are handled securely.

8. Retention and archiving

- 8.1 Users should routinely archive and delete unnecessary emails.

9. Reporting security incidents

- 9.1 Any suspected breach, loss of a device, unauthorised access or other security incident must be reported immediately to the clerk or chair.

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	Approval Minute
1	Mar 2026	Initial adoption of policy.	TBC