Dilton Marsh Parish Council

Communications, IT and Cyber Security Policy

Adopted at a meeting of the Parish Council held on 20th November 2025

1. Introduction

1.1 Dilton Marsh Parish Council has a duty to ensure the proper security and privacy of its information and data. All Councillors and employees are responsible for protecting such information and are to comply with this policy.

1.2 The Parish Clerk is responsible for monitoring this policy and for ensuring that it is reviewed annually.

2. General Principles

2.1 The default mechanisms for Dilton Marsh Parish Council to communicate are email, the Council website and the Council Facebook site. This reduces costs and helps to maintain configuration control of documents and information.

2.2. Only in exceptional circumstances, such as a response to a Freedom of Information or Subject Access Request, will the Council produce hard copy communications material. In such cases, the printed information is classed as 'uncontrolled'. Reasonable printing/reproduction costs may be recovered from individuals requesting information in hard copy.

2.3 All Councillors and the Parish Clerk are responsible for ensuring the security and integrity of Parish Council Information by observing good practice concerning cyber security.

2.4 The Parish Council has a separate Data Protection Policy which should be read in conjunction with this document.

3. IT Hardware and Cyber Security

3.1 Dilton Marsh Parish Council does not provide End User Devices for use by Councillors and employees. Users should use their own Laptops/Desktops/Tablets and take proper precautions to ensure that Council information is protected. These precautions need not be more onerous than normal, best practice for protecting any personal information and should include:

a. **Current Software and Operating Systems**. Users should avoid using obsolete software and operating systems. The latter represent a particular risk as they are not maintained or 'patched' to counter new and emerging cyber threats.

b. **Anti-Virus protection software**. Where appropriate, anti-virus protection software should be installed and/or activated.

b. **Strong Passwords**. Users should ensure that their devices require a password for access, and that they employ 'strong passwords'.

c. **Multi-Factor Authentication and Biometrics**. Where available, Users should enable Multi-Factor authentication and Biometrics in addition to using strong passwords.

d. **Hard Disc Encryption**. Most current operating systems include optional hard encryption and this should be enabled where available.

e. **WiFi Access**. Users should not access public WiFi networks without using a Virtual Private Network.

4. email Correspondence

4.1. Councillors and employees should not use private email accounts for Council business. This is because all emails relating to Council business are considered Council data. email accounts containing such data are subject to UK Data Protection and FOI legislation and full access to those accounts may be required by external authorities.

4.2. The Parish Clerk is to arrange for all members of the Council to have official, diltonmarshparishcouncil.gov.uk email accounts.

4.3. The Parish Clerk is responsible for disabling official email accounts when Councillors step down.

4.4. All Councillors and employees should remain vigilant regarding cybersecurity threats. Suspicious activity or emails should be reported to the Parish Clerk. Users should never share passwords via email and should be cautious of odd or inconsistent language in communications.

4.5. Councillors should use their own judgement when copying correspondence to other members. All emails from Councillors to the Parish Clerk should be copied to the Council Chair.

5. Website and Social Media.

5.1 The Parish Clerk is responsible for the maintenance of the Council website and for ensuring that all necessary documents, reports, agendas and minutes are published promptly.

5.2 The Parish Clerk is responsible for the Council Facebook site. In addition, nominated Councillors may post Council information on the site.

5.3. Posts on the Parish Council website and Facebook site must be apolitical, factual, and in the interests of the parish

5.4. When using any social media in a personal capacity, members must not refer to Parish Council business or policy.

……

Chair