The Orchards' and Margaret Marsh Parish Council

INFORMATION TECHNOLOGY (IT) POLICY

1. Purpose

The Parish Council uses information technology to manage its work, communications, and records. This policy sets out how those systems are used and protected, ensuring that information is handled securely and in accordance with legal requirements. This policy should be read alongside the Council's Data Protection Policy and Financial Regulations

2. Scope

This policy applies to all Council IT systems and data, including laptops, email, cloud storage, and any devices used for Council business.
As the sole employee, the Parish Clerk is the primary user of these systems and is responsible for their secure and appropriate use.

3. Use of IT Systems

Council IT systems are to be used for official Council business. Reasonable personal use is acceptable where it is occasional and does not interfere with Council duties or compromise security.
Systems must not be used in any way that is unlawful, inappropriate, or could expose the Council to risk—such as accessing inappropriate material, introducing unauthorised software, or attempting to bypass security controls.

4. Data Protection and Security

The Council processes information in accordance with its Data Protection Policy and relevant legislation.
The Clerk is responsible for ensuring that information is stored securely using approved systems, that personal data is only accessed where necessary, and that confidential information is protected and not disclosed without appropriate authority. Where possible, Council data should not be stored on personal devices.

5. Access and Password Security

Access to systems is controlled by secure passwords and Multi-Factor Authentication (MFA) that must not be shared. Users are expected to follow good practice in maintaining strong passwords and to update them if there is any concern that they may have been compromised.

6. Equipment and Remote Working

The Council provides a laptop equipped with the Microsoft 365 Business package, which is covered by the Council's insurance policy. Reasonable care must be taken to prevent loss, damage, or unauthorised access, particularly when equipment is used outside the home.

7. Email and Communication

Email is a formal communication channel for the Council. Messages are treated as part of the official records and can be requested as part of any Freedom of Information request.

- Messages should be constructed in a professional and considered manner, and users should avoid making commitments or statements beyond their delegated authority.
- Users should remain alert to risks such as phishing emails or fraudulent communications.
- While communication methods such as text messaging or messaging apps may be used for convenience, they should not be relied upon for formal decision-making or record-keeping.

8. Internet and Software Use

Software should only be installed where authorised, and systems should be kept up to date to ensure security and performance.

9. Website and External Systems

The Parish Council uses externally hosted systems to support its operations, including its website and domain management. These services are provided by a third-party supplier and accessed via a secure online portal.

- The Clerk manages access to these systems and ensures login credentials are kept secure. To maintain continuity, important access details will be stored securely and provided to the Chair in case of absence or emergency.
- The Council's use of a .gov.uk domain supports enhanced security and public trust, and systems will be maintained in line with good practice.

10. Communication and Informal Channels

The Parish Council does not operate official social media accounts.

- Information may occasionally be shared via community channels or messaging groups to enhance local awareness, particularly regarding meetings or urgent issues such as flooding. Such communications are supplementary and do not replace formal Council notices, agendas, or minutes.
- Care is taken to ensure that any information shared is appropriate and that personal views are not mistaken for official Council positions.

11. Risk Awareness

The Clerk will remain aware of common IT risks, including phishing emails, data breaches, and unauthorised access, and will take reasonable steps to mitigate them. Any suspected security issue or data breach must be addressed promptly and, where appropriate, reported to the Council.

12. Adoption

This policy was reviewed and adopted by The Orchards and Margaret Marsh Parish Council at the meeting held on 18th May 2026

13. Review

This policy will be reviewed annually, or sooner if there are significant changes to systems, risks, or legal requirements. Date of next review: May 2027.

No	Change Type	Updated By	Change Summary	Approval Date
1	Original	OMMPC	Adopted	18/5/2026
			Next review	5/2027

Signed: Date: 18th May 2026.
Chair, The Orchards' and Margaret Marsh Parish Council

14. Sources and References

NALC IT Policy resources
Freedom of Information Act 2000 (FOIA)
Data Protection Act 2018
UK General Data Protection Regulation (UK GDPR)
Computer Misuse Act 1990
Environmental Information Regulations 2004 (EIR)
Privacy and Electronic Communications Regulations 2003 (PECR)
Electronic Communications Act 2000