Lympstone Parish Council

Information Technology (IT) Policy

1. Introduction and Purpose

This policy establishes the rules for the secure and appropriate use of Lympstone Parish Council's Information Technology (IT) systems and data. Its purpose is to:

- Ensure all Users understand their responsibilities.
- Protect the Council's IT equipment, systems, and data from loss, misuse, or theft.
- Safeguard the privacy of councillors, employees, parishioners and third parties.
- Ensure compliance with relevant UK legislation, including data protection, freedom of information, and accessibility laws.
- All councillors are entitled to be issued with an iPad – but this should only be used for Council use.

The policy part of the Council's risk management and serves as our primary defence against IT-related incidents such as data breaches, cyber-attacks, and legal non-compliance.

For further clarification or information on this policy, please contact the Clerk to the Council at: clerk@lympstoneparishcouncil.gov.uk

2. Definitions

- **Users:** All councillors, employees, contractors, and volunteers acting on behalf of the Council as well as third parties.
- **Data:** Any digitally stored information, including but not limited to documents, emails, images, personal data, and financial records.
- **IT Systems:** All council-owned or managed hardware and software, including computers, laptops, mobile phones, servers, internet access, email accounts, cloud storage, and the Council website.

3. Scope

This policy applies to all Users and covers the use of all IT resources (including computers, networks, devices, data and email), whether accessed on council premises, remotely, or from personal devices when used for council business.

4. **Acceptable Use of IT Systems**
    - **Council Business Only:** IT systems are provided for official council business only. Personal use is strictly prohibited.
    - **Authorised Use:** Users must not access data or software they are not authorised to use. Unauthorised changes to systems or data are forbidden.
    - **Software:** Users must not install unauthorised software on council equipment. Clarification on approved software can be sought from the Clerk.
    - **Return of Equipment:** All council equipment must be returned to the Clerk, Chairman, or Vice-Chairman upon the end of a term of office, employment, or contract. A charge may be levied for lost or damaged equipment.

5. **Council Email and Communication**
    - **Official Email Address:** The Council will provide an official email address (e.g., name@lympstoneparishcouncil.gov.uk) to all councillors and employees. This must be used for all council correspondence, both official and unofficial.
    - **No Personal Email for Business:** To comply with Data Protection regulations and to prevent lost emails when personnel change, Users are prohibited from using personal email accounts (e.g., Gmail, Hotmail) for council business.
    - **Email Footers:** The standard disclaimer should be added to all outgoing emails to external parties (see appendix A below or ask the Clerk/RFO to provide)
    - **Record Keeping:** Any correspondence undertaken on behalf of the Council (on council or personal devices) is a council record and must be provided to the Clerk upon request, especially in relation to Freedom of Information (FOI) requests. It is good practice that the Clerk and Chair is CC'd BC'd in to all correspondence.
    - **Network and internet usage:** Users must be careful about which Wi-Fi networks they join. Public Wi-Fi networks in coffee shops or on trains can be targeted by hackers. Always make sure that a trusted internet connection is used and is password protected when carrying out official business.

6. **Passwords and Access Control**
    - **Password Strength:** Strong passwords must be used. Usually, a combination of 2 or more words or generated by a password generator.
    - **Two-Factor Authentication (2FA):** Where available, 2FA **must** be enabled, using a hardware key or an authenticator app (e.g., Google Authenticator).
    - **Password Log:** For business continuity, essential passwords must be securely logged with the Clerk.
    - **Biometric Authentication:** On council-provided devices, biometric authentication (e.g., fingerprint, facial recognition) should be activated under a council-managed account.

7. Data Protection and Information Security

Users must comply with UK Data Protection regulations.

- **Data Sharing:** Council data or software must not be transferred to any external person or organisation without proper authority.
- **Secure Storage:** Data must be stored and accessed only via council-approved, secure methods. Personal data must not be stored on unencrypted USB sticks, personal cloud services, or personal devices unless explicitly authorised.

8. Website Management and Legal Compliance

The Council website is a public-facing system and must be managed professionally.

- **Transparency:** All required documents (minutes, agendas, financial information, councillor details) must be published promptly in accordance with the Transparency Code.
- **Accessibility**: The Website meets the Public Sector Bodies (Website Mobile Applications (no.2) Accessibility Regulations.
- **FOI Requests:** Freedom of Information requests received via the website or any other channel must be handled in accordance with the Council's FOI procedure and legal timelines.

9. Cybersecurity and Risk Management

The Council will take proactive steps to defend against cyber-attacks such as phishing and malware.

- **Insurance and Security:** Equipment is insured, but Users must take practical steps to secure it from theft or unauthorised use. Devices must not be left in unattended vehicles and must be secured out of sight.
- **Incident Reporting:** Any loss, damage, or criminal activity involving IT equipment must be reported immediately to the Clerk and Chairman.
- **Vigilance:** Users must be vigilant against suspicious emails (phishing). Do not click links or open attachments from unknown senders. Suspected phishing attempts must be reported to the Clerk.
- **Annual Risk Assessment:** An annual risk assessment of the Council's IT hardware, software, and data security will be conducted.

10. Social Media and Online Conduct

- **Official Accounts:** Only authorised personnel may post on the Council's official social media accounts.
- **Personal Accounts:** Councillors and staff must make it clear when expressing personal views online that they are not speaking on behalf of the Council. Professional conduct is expected at all times.

11. Policy Review and Training

- **Review Cycle:** This policy will be reviewed **annually**, or upon a significant change in IT systems or legislation. A review will also be triggered within three months of new staff starting or following council elections.
- **Training:** All Users will be offered training on this policy, data protection, and IT security best practices to ensure ongoing compliance and awareness.

Initial policy adopted: 6th July 2026

Updated: 6th July 2026 Minute Reference: 26/56.2

Next review: July 2027

Appendix A – Disclaimer Wording

Email disclaimer: http://www.lympstone.org/wp-content/uploads/2018/04/Web-email-disclosure.pdf

DISCLAIMER

This message is intended only for the use of the person(s) ("Intended Recipient") to whom it is addressed. It may contain information, which is privileged and confidential. Accordingly, any dissemination, distribution, copying or other use of this message or any of its content by any person other than the Intended Recipient may constitute a breach of civil or criminal law and is strictly prohibited. If you are not the Intended Recipient, please contact the sender as soon as possible.