LENHAM
PARISH COUNCIL

Controlled Document

Title	IT Policy
Author	Lenham Parish Council
Owner	Lenham Parish Council
Subject	Main Policy Documents
Government Security Classification	Official
Document Version	Version 1.01
Created	13.10.2025
Approved By	Full Council
Review Date	4.11.2026

Version Control

Version	Date	Author	Description of Change	Sign
1	**5.11.2025**	**Lenham Parish Council**	**Original Policy**	**L.Westcott**

IT Policy

Introduction

Lenham Parish Council (the Council) recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications.
This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by council members, employees, volunteers and contractors.

It complies with the Data Protection Act 2018 (DPA 2018), UK General Data Protection Regulation (UK GDPR), and the Data (Use and Access) Act 2025 (DUAA).

Scope

This policy applies to all individuals who use the Council's IT resources including computers, networks, software, devices, data and email accounts.

Acceptable use of IT resources and email

The Council's IT resources and email accounts are to be used for official Council-related activities and tasks. Limited personal use is permitted, provided it does not interfere with work responsibilities or violate any part of this policy. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

Under DUAA 2025, use of data for public benefit is encouraged, but must be secure and compliant.

Device and software usage

Where possible, authorised devices, software and applications will be provided by the Council for work-related tasks.

Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

Data Management and security

All sensitive and confidential Lenham Parish Council data should be stored and transmitted securely using approved methods. Regular data backups should be performed to prevent data loss, and secured data destruction methods should be used when necessary.

DUAA 2025 allows for more flexible data use in smart schemes, but we must ensure data is protected against unauthorised access.

Network and internet usage

Lenham Parish Council's network and internet connections should be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited.

Email communications

Email accounts provided by Lenham Parish Council are for official communications only. Emails should be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless it is encrypted.

Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

An email signature should be used in line with the Council's agreed format.

Password and account security

Lenham Parish Council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others. Regular password changes are encouraged to enhance security.

Remote working

When working remotely, users should follow the same security practices as if they were in the office.

Email monitoring

Lenham Parish Council reserves the right to monitor email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with DPA 2018, UK GDPR, and DUAA 2025 (as applicable to data access and use).

Retention and archiving

Emails should be retained and archived in accordance with legal and regulatory requirements. Email inboxes should be reviewed regularly and unnecessary emails deleted. This is essential to maintain an organised inbox and ensure the mailbox does not reach its limit.

Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the Clerk, who is the designated IT point of contact for investigation and resolution. Report any email-related security incidents or breaches to the clerk immediately.

Training and awareness

Lenham Parish Council provides regular resources to educate users about IT security best practices, privacy concerns and technology updates. All employees and Councillors will receive appropriate training on email security and best practice, including DUAA 2025 implications for data sharing.

Compliance and consequences

Breach of this IT policy may result in the suspension of IT privileges and further consequences as deemed appropriate.

Policy review

This policy will be immediately reviewed upon finalisation of the DUAA act 2025 (expected around Feb 2026), and subsequent reviews will be completed annually to ensure its relevance and effectiveness.

Updates may be made to address emerging technology trends and security measures.

Contacts

For IT-related enquiries or assistance, users can contact the Clerk. All staff and Councillors are responsible for the safety and security of Lenham Parish Council's IT systems. By adhering to this IT Policy, the Lenham Parish Council aims to create a secure and efficient IT environment that supports its mission and goals.