

Leckhampstead Parish Council

Information Technology and Email Policy

1. Introduction

Leckhampstead Parish 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.

2. Scope

This policy applies to all individuals who use Leckhampstead Parish Council IT resources, including computers, networks, software, devices, data, and email accounts. It also applies to all computers, software, data, devices and email accounts which belong to or are used by Council members.

3. Acceptable use of IT resources and email

Leckhampstead Parish Council 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 and Council members must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

4. Device and software usage

Where possible, authorised devices, software, and applications will be provided by Leckhampstead Parish Council for work-related tasks. Council members are also permitted to use their own devices, software and email accounts provided they comply with the terms of this policy.

All devices must have appropriate and up to date anti-virus and anti-malware software.

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

5. Data management and security

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

6. Network and internet usage

Internet connections should be used responsibly and efficiently for official purposes. Home Wi-Fi networks must be encrypted and care should be exercised if using public Wi-Fi to connect Devices.

Downloading and sharing copyrighted material without proper authorisation is prohibited.

7. Email communication

Email accounts provided by Leckhampstead Parish Council are for official communication only.

All emails sent in connection with Leckhampstead Parish Council business 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.

8. Password and account security

Leckhampstead Parish Council users and council members 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.

9. Mobile devices

Any mobile device used in connection with Leckhampstead Parish Council business should be secured with passcodes and/or biometric authentication.

10. Email monitoring

Leckhampstead 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 the Data Protection Act and GDPR.

11. Retention and archiving

Emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an organised inbox.

12. Reporting security incidents (including devices lost or stolen)

All suspected security breaches including any email related security incident should be reported immediately to the Parish Clerk for investigation and action, including reporting matters to the Information Commissioners Office (ICO) if a breach of any personal data is identified

In the event that a Device is lost or stolen, or is suspected of having been lost or stolen, the Parish Clerk must be informed immediately. The Parish Council will work with the owner of the lost or stolen Device to identify any personal data at risk and will then take appropriate action, including reporting any breach to the ICO as necessary.

13. Leaving the Parish Council

If a Councillor ceases to be a member of the Parish Council for any reason: (a) all Personal Data received in the course of Parish Council Business must be permanently deleted from their own devices and from any email account used for Parish Council Business; and (b) all hard copies should be shredded or passed to the Clerk for destruction.

On the termination of the Clerk's employment by the Parish Council: (a) the Clerk must return Devices issued by the Parish Council immediately; and (b) all Personal Data or other information received in the course of Parish Council Business must be permanently deleted from personally owned Devices.

14. Compliance and consequences

Breach of this IT and Email Policy may result in the suspension of IT privileges and further consequences as deemed appropriate, including disciplinary action.

15. Policy review

This policy will be reviewed annually to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures at any time.

By adhering to this IT and Email Policy, [Leckhampstead Parish Council aim to create a secure and efficient IT environment that supports its mission and goals.

Date of policy: 1st September 2025

Date of Adoption by the Council: 24th February 2026

Date for next review: May 2027