Lutton Parish Council Smaller Authorities IT Policy

1. Introduction

Lutton Parish Council henceforth known as "The Authority" 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 IT resources, including computers, networks, software, devices, data, and email accounts. The authority endeavours to provide digital devices but acknowledges that some small authority staff and members may be using their own personal devices. Everyone must adhere to this policy to maintain digital security.

3. Training and awareness

The Authority will source regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. You should engage in regular training on email security and best practices, including but not limited to:

- the Parish Council Domain Helper Service's virtual cybersecurity workshops for councils

- The National Cyber Security Centre Cyber Security training for small organisations and free Cyber Action Toolkit.

4. Acceptable use of council provided IT resources and email

When using IT resources for the council's purposes, you must adhere to ethical standards, and respect copyright and intellectual property rights.

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

You must not install unauthorised software without checking with the clerk, and you must not use equipment or email to access or forward inappropriate or offensive content.

5. What you must do if you use your own personal devices

The Authority will endeavour to provide individuals with devices to use for council business. If you are using your own device you must make sure you are:

- using strong passwords for all your accounts (preferably using a password manager)
- downloading the latest operating system security updates
- using anti-virus software

6. Network and internet usage

You must be careful about which Wi-Fi networks you join. Public Wi-Fi networks in coffee shops or on trains can be targeted by hackers. Always make sure you are using a trusted internet connection, which is password protected when carrying out official business.

7. Password and account security

You are responsible for maintaining the security of your accounts and passwords. Use the National Cyber Security Centre's advice for choosing a strong password. For business continuity, login details and passwords need to be stored securely so they can be accessed by trusted individuals in an emergency.

8. Email communication

The Authority will endeavour to provide you with an official email account for organisation-related communication only. If you are currently using a personal email account, you should aim to move over to an official email account as soon as practically possible. You must make sure that emails are professional and respectful in tone. You must always check you are sending any confidential or sensitive information to the correct recipients.

Always be cautious when downloading attachments and opening links to avoid phishing and malware. Before opening any attachments or clicking on links, verify

the source by looking at the email it has come from carefully. Do not download and open anything if you are unsure who has sent it.

9. Email access

The Authority reserves the right to check email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR. Clerks may need to access emails so that they respond to FOI or subject-access requests. If you are using a personal email account for council business, this is still subject to data protections laws and FOI requests.

10. Data management, data retention and security

All sensitive and confidential data should be stored and transmitted securely. You must regularly backup any important data to prevent data loss and follow your organisation's data retention policies.

You should retain and archive emails in compliance with your data retention policies. Regularly review and delete unnecessary emails to maintain an organised inbox.

11. Reporting security incidents

All suspected security breaches, including email breaches or incidents should be reported immediately to the Clerk.

12. Compliance and consequences

Breach of this IT and Email Policy may result in the suspension of IT privileges.

13. 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.

14. Contacts

For IT-related enquiries or assistance, users can contact the Clerk.

All staff and councillors are responsible for the safety and security of IT and email systems.

Date of adoption: at a meeting of the authority on **18th May 2026**

Date for next review: May 2027