

LILBOURNE PARISH COUNCIL IT POLICY

Version Control	Purpose / Change	Author	Date
1.0	First published	Lilbourne Parish Council	February 2026

National Cyber Security Centre

Table of Contents

1. Introduction 3

2. Scope 3

3. Training and Awareness 3

4. Acceptable use of Council provided IT resources and Email 4

5. What individuals must do if using own personal devices 4

6. Network and Internet usage 4

7. Password and Account Security 4

8. Email Communication 5

9. Email Access 5

10. Data Management, Data Retention and Security 5

11. Reporting Security Incidents 6

12. Compliance and Consequences 6

13. Policy Review 6

14. Contact 6

15. Adoption of Policy 6

1. Introduction

1.1 Lilbourne 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.

1.2 This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by council members, employees, volunteers and contractors.

1.3 The policy has been written taking into account best practice and guidance as circulated by the National Cyber Security Centre.

2. Scope

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

2.2 The Authority endeavours to provide digital devices to those individuals but acknowledges that some Authority staff and members may be using their own personal devices.

2.3 Everybody must adhere to this policy to maintain digital security .

3. Training and Awareness

3.1 The Authority will source regular training and resources to educate users about IT security best practices, privacy concerns and technology updates.

3.2 Individuals should engage in regular training on email security and best practices, including but not limited to:

3.2.1 The Parish Council Domain Helpers Services virtual cybersecurity workshops for councils

3.2.2 The National Cyber Security Centre – Cyber Security Training for Small Organisations and,

3.2.3 The free Cyber Action Toolkit

National Cyber Security Centre

4. Acceptable use of Council provided IT resources and Email

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

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

4.3 Individuals must not install unauthorised software without checking with the Clerk, and must not use equipment or email to access or forward inappropriate or offensive content.

5. What individuals must do if using own personal devices

5.1 The Authority will endeavour to provide individuals with devices to use for council business.

5.2 If individuals are using their own devices, individuals must:

5.2.1 Use strong and unique passwords for all accounts (preferably using a password manager)

5.2.2 Ensure devices are fully supported by the manufacturer

5.2.3 Download the latest operating system security updates as soon as available, preferably within 14 days of release.

5.2.4 Use updated and supported anti-virus software.

6. Network and Internet usage

6.1 Individuals must be careful about which Wi-Fi networks to join.

6.2 Public Wi-Fi networks in coffee shops or on trains can be unsafe to use.

6.3 Only trusted internet connections should be used which are password protected when carrying out official business.

7. Password and Account Security

7.1 Individuals are responsible for maintaining the security of your accounts and passwords. Use the National Cyber Security Centre's – Advice for choosing a strong password.

7.2 Where available, multi-factor authentication (MFA) must be used to enhance account security.

7.3 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

8.1 The Authority will endeavour to provide individuals with an official email account for Parish Council related communication only.

8.2 If individuals are currently using a personal email account, this should be moved to an official email account as soon as practically possible.

8.3 Individuals must make sure that emails are professional and respectful in tone.

8.4 Confidential or sensitive information must be checked to ensure accuracy of information and correct recipient(s).

8.5 Always be cautious when downloading attachments or clicking links; verify the source by looking at the email it has come from carefully.

8.6 Do not download or open any files or attachments that may seem suspicious.

9. Email Access

9.1 The Authority reserves the right to check email communications to ensure compliance with this policy and relevant laws.

9.2 Monitoring will be conducted in accordance with the Data Protection Act and GDPR.

9.3 Clerks may need to access emails so that they respond to Freedom of Information (FOI) Act subject-access requests.

9.4 If individuals are using a personal email account for council business, this is still subject to data protection laws and FOI Requests.

10. Data Management, Data Retention and Security

10.1 All sensitive and confidential data should be stored and transmitted securely

10.2 Individuals must regularly back up and archive any important data, including emails, to prevent data loss and follow the Authority's data retention policies.

National Cyber Security Centre

10.3 Regularly review and delete unnecessary emails to maintain an organised inbox.

11. Reporting Security Incidents

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

11.2 for further information or contact the Clerk to the Parish Council if you cannot access the internet.

12. Compliance and Consequences

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

13. Policy Review

13.1 This policy will be reviewed annually to ensure its relevance and effectiveness.

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

14. Contact

14.1 For IT-related enquiries or assistance, individuals can contact the Clerk to the Parish Council.

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

15. Adoption of Policy

15.1 Date of Adoption:……at a meeting of the Authority on ……(include link to minute reference)

15.2 Date of next review:……

National Cyber Security Centre