CLIPSTON PARISH COUNCIL

c/o 20 Styles Place, Yelvertoft, Northamptonshire, NN6 6LR
Email: clerk@clipstonparishcouncil.org
Website: http://www.clipstonparishcouncil.gov.uk

IT Policy

Version Control

Version	Purpose / Change	Author	Date
1.0	First published	Clipston Parish Council	[March 2026]

Table of Contents

1. Introduction

1.1 Clipston Parish Council ("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 sets out the guidelines and responsibilities for the appropriate use of IT resources and email by councillors, employees, volunteers, and contractors.

1.3 The policy is informed by best practice and guidance issued by the **National Cyber Security Centre (NCSC)**.

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 aims to provide digital devices for council business but acknowledges that some individuals may use their own personal devices.

2.3 All individuals must adhere to this policy to maintain digital security.

CLIPSTON PARISH COUNCIL

c/o 20 Styles Place, Yelvertoft, Northamptonshire, NN6 6LR
Email: clerk@clipstonparishcouncil.org
Website: http://www.clipstonparishcouncil.gov.uk

3. Training and Awareness

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

3.2 Individuals should engage in regular training, including:

- NCSC Cyber Security Training for Small Organisations
- NCSC Cyber Action Toolkit
- Parish-sector cybersecurity workshops

4. Acceptable Use of Council-Provided IT Resources and Email

4.1 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 for council work.

4.3 Individuals must not install unauthorised software and must not use council equipment or email to access or forward inappropriate or offensive content.

5. Requirements When Using Personal Devices

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

5.2 If personal devices are used, individuals must:

- Use strong, unique passwords (preferably with a password manager)
- Ensure devices are fully supported by the manufacturer
- Install operating system updates promptly (ideally within 14 days)
- Use supported and up-to-date antivirus software

6. Network and Internet Usage

6.1 Individuals must be cautious when selecting Wi-Fi networks.

6.2 Public Wi-Fi (e.g., cafés, trains) may be unsafe.

6.3 Only trusted, password-protected networks should be used for council business.

7. Password and Account Security

7.1 Individuals are responsible for maintaining the security of their accounts and passwords.

7.2 Multi-factor authentication (MFA) must be used where available.

7.3 Login details must 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 official email accounts for council business.

8.2 Personal email accounts should be phased out for council use as soon as practicable.

8.3 Emails must be professional and respectful.

8.4 Sensitive information must be checked for accuracy and correct recipients.

8.5 Be cautious with attachments and links; verify the sender.

8.6 Do not open suspicious files or attachments.

CLIPSTON PARISH COUNCIL

c/o 20 Styles Place, Yelvertoft, Northamptonshire, NN6 6LR
Email: clerk@clipstonparishcouncil.org
Website: http://www.clipstonparishcouncil.gov.uk

9. Email Access
9.1 The Authority reserves the right to check email communications to ensure compliance with this policy.
9.2 Monitoring will comply with the Data Protection Act and GDPR.
9.3 Clerks may need access to emails to respond to FOI or subject access requests.
9.4 Personal email accounts used for council business remain subject to FOI and data protection laws.

10. Data Management, Data Retention and Security
10.1 All sensitive and confidential data must be stored and transmitted securely.
10.2 Individuals must regularly back up important data and follow the Authority's retention policies.
10.3 Unnecessary emails should be regularly reviewed and deleted.

11. Reporting Security Incidents
11.1 All suspected security breaches, including email breaches, must be reported immediately to the Clerk.
11.2 If internet access is unavailable, individuals should contact the Clerk by alternative means.

12. Compliance and Consequences
12.1 Breach of this policy may result in suspension of IT privileges.

13. Policy Review
13.1 This policy will be reviewed annually.
13.2 Updates may be made to reflect emerging technology and security measures.

14. Contact
14.1 For IT-related enquiries, individuals should contact the Clerk.
14.2 All staff and councillors share responsibility for IT and email security.

15. Adoption of Policy
15.1 Date of Adoption:

Adopted at a meeting of Clipston Parish Council on: _____March 2026_____
(Minute reference: _____)

15.2 Date of next review: _____May 2027_____