Clipstone Parish Council

Clipstone Parish Council IT Policy

---

1. Introduction

Clipstone Parish Council (the Council) is committed to ensuring that its Information Technology (IT) infrastructure, systems, and data are secure, efficiently managed, and used responsibly. This IT Policy outlines the practices and guidelines for the use of the Council's IT systems, in line with the standards set by the **SAAA** (Smaller Authorities' Audit Appointments) guidelines and **NALC** (National Association of Local Councils) model template. It aims to protect both the Council's and individuals' data and to ensure compliance with relevant legislation and regulations.

---

2. Purpose of the Policy

The purpose of this IT Policy is to:

- Protect the integrity and confidentiality of the Council's data and IT systems.
- Provide clear guidelines for the responsible use of IT resources.
- Ensure compliance with legal and regulatory obligations, including data protection laws (GDPR).
- Promote a secure and efficient IT environment for all users.

---

3. Scope of the Policy

This policy applies to:

- All Council employees, members, contractors, and volunteers who use the Council's IT systems and resources.
- All IT equipment, including computers, software, mobile devices, networks, and data storage.
- Any remote or external access to the Council's IT systems, including access through home working arrangements or cloud-based services.

---

4. Responsibilities

- **Council Members and Employees**: Must comply with the terms of this policy and report any breaches, vulnerabilities, or issues promptly.

- **Clerk**: Responsible for ensuring that all Council members and employees are trained on IT usage and security protocols.

---

5. Acceptable Use of IT Resources

IT resources are provided to assist in the effective management and operation of Council business. All users of the Council's IT systems are expected to follow these guidelines:

- **Authorised Use Only**: IT systems and resources should only be used for official Council business. Personal use should be kept to a minimum and not interfere with work duties.
- **Software Usage**: Only legally licensed software and applications may be used. Installation of non-approved or illegal software is prohibited.
- **Access Control**: Access to systems, networks, and files should be restricted based on job roles. Sensitive data should only be accessible to authorised users.
- **Internet Use**: Internet usage should be for business purposes only. Personal browsing, social media, or activities unrelated to Council work are not permitted during working hours.

---

6. Data Protection and Confidentiality

In line with **GDPR** and other relevant legislation, the following guidelines must be adhered to:

- **Data Protection**: Personal data (e.g., employee records, councillor details, etc.) must be processed fairly and lawfully. Data should only be accessed when necessary for official business purposes.
- **Confidentiality**: All confidential information, whether related to personnel, finances, or other aspects of the Council's operations, must be handled with care and kept secure. Unauthorised disclosure of sensitive information is prohibited.
- **Data Storage**: All Council data should be stored in secure locations, whether on physical devices or cloud services, and must be encrypted where necessary.
- **Data Retention**: Data should only be kept for as long as necessary. All documents should be regularly reviewed, and obsolete or unnecessary data should be securely deleted.

---

7. Security of IT Systems

The Council’s IT systems must be safeguarded against threats such as unauthorised access, cyber-attacks, and data loss. The following practices are essential:

- **Password Security**: All users must employ strong passwords and change them regularly. Passwords must never be shared with others.
- **Antivirus Software**: All computers and devices must have up-to-date antivirus software installed to prevent malware and other threats.
- **Backup**: Regular backups of critical Council data must be performed.
- **Software Updates**: All devices and systems should have the latest security patches and updates installed to mitigate vulnerabilities.

---

8. Email and Communication

- **Email Use**: Official Council email accounts should be used for all formal communications. Personal email accounts should not be used for Council business.
- **Phishing and Suspicious Emails**: Users should be vigilant against phishing attacks and suspicious emails. Emails from unknown senders or with unexpected attachments should be treated with caution.
- **Email Retention**: Emails containing sensitive or personal data should be securely archived or deleted once they are no longer required.

---

9. Social Media and Public Communication

Council members and employees should be cautious when engaging with social media platforms, both in a personal and professional capacity. The following guidelines should be followed:

- **Official Accounts**: Only designated individuals (such as Council staff and any approved Councillors) may post or engage on behalf of the Council through official social media accounts.
- **Personal Accounts**: Council members should ensure their personal social media profiles do not create conflicts of interest or damage the reputation of the Council.

---

10. Remote Working and Homeworking

For users working remotely, the following protocols must be followed:

- **Device Security**: Devices used for remote work must be encrypted, protected by strong passwords, and have up-to-date antivirus software.
- **Data Handling**: All data accessed remotely should be stored and processed in compliance with the Council’s data protection policy.

---

11. Incident Reporting and Breaches

Any breach or suspected breach of this IT Policy must be reported immediately to the Clerk. The Council will investigate all incidents, including:

- Unauthorised access to IT systems.
- Loss, theft, or unauthorised disclosure of data.
- Cyber-attacks or malware infections.

The Council will take appropriate action to address and mitigate any incidents. Repeated violations or serious breaches may result in disciplinary action.

---

12. Policy Review

This IT Policy will be reviewed annually to ensure that it remains up-to-date with changes in technology, legal requirements, and best practices. Any amendments or updates to the policy will be communicated to all Council members and staff.

---

13. Enforcement

Failure to comply with this policy may result in disciplinary action, including loss of IT access privileges or further disciplinary measures as determined by the Council.

---

14. Approval

This policy was approved by Clipstone Parish Council on 28 May 2025

Agenda Item: CPC25/26 19a

Signed: D Edkriett

By following this policy, Clipstone Parish Council ensures the effective, secure, and responsible use of IT resources, promoting efficiency and compliance with all relevant standards and regulations.