

Chilton Polden Parish Council

IT and Communications Policy

Adopted: _____

Review Date: Annually

Contents

Introduction

Scope

Acceptable Use of IT Resources

Use of Council Email Accounts

Passwords and Account Security

Device, Software and Network Usage

Data Management and Security

Monitoring of IT Systems and Email

Retention and Archiving

Security Incidents and Data Breaches

Use of Mobile Devices and Remote Working

Software and System Security

Council Website and Social Media

Training and Awareness

Compliance and Consequences

Policy Review

Contacts

1. Introduction

1.1 This policy sets out the requirements for the acceptable use, management, and security of information technology systems used by Chilton Polden Parish Council.

1.2 The policy aims to ensure that the Council's IT systems, electronic communications, and data are used responsibly, securely, and in compliance with statutory obligations.

1.3 This policy supports compliance with:

UK GDPR

Data Protection Act 2018

Relevant guidance issued by the National Association of Local Councils (NALC)

2. Scope

2.1 This policy applies to parish councillors, the Parish Clerk, council employees, volunteers, contractors, and any authorised persons who have access to council IT systems or information.

2.2 The policy covers:

Council email systems

Computers and IT equipment owned by the Council

Mobile devices used for council business

Data storage and backups

Networks and internet access

Council website and social media platforms

Remote access to council systems

3. Acceptable Use of IT Resources

3.1 Council IT resources and email accounts are provided primarily for official council business and activities.

3.2 Limited personal use may be permitted provided it:

Does not interfere with council duties or operations

Does not incur unreasonable cost

Does not breach this policy or any legislation

3.3 Users must:

Use council IT systems responsibly and lawfully

Adhere to ethical standards

Respect copyright and intellectual property rights

Avoid accessing or distributing inappropriate, offensive, or illegal material

3.4 The following activities are strictly prohibited:

Downloading or sharing copyrighted material without authorisation

Installing unauthorised software on council-owned devices

Accessing or distributing offensive, inappropriate, or illegal content

Using council IT systems for unlawful, fraudulent, or improper purposes

4. Use of Council Email Accounts

4.1 Council email addresses shall be used for official parish council business.

4.2 Users must ensure that all email communications are professional, respectful, and appropriate to the public role of the Council.

4.3 Email communication must comply with professional standards and guidance issued by the National Association of Local Councils.

4.4 Users must exercise care when sending emails and ensure messages are sent only to appropriate recipients.

4.5 Confidential or sensitive information must not be transmitted via email unless appropriate safeguards are in place, including encryption where necessary.

4.6 Users should remain vigilant against phishing emails, malicious attachments, and suspicious links, and should verify the source of emails before opening attachments or clicking links.

5. Passwords and Account Security

5.1 All council IT systems, devices, and email accounts must be protected by secure passwords.

5.2 Users must:

Use strong passwords

Keep passwords confidential

Not share passwords with unauthorised individuals

Lock or log out of devices when unattended

Report suspected unauthorised access immediately to the Parish Clerk

5.3 Where possible, additional security measures such as two-factor authentication should be used.

5.4 Regular password changes are encouraged to enhance security.

6. Device, Software and Network Usage

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

6.2 Unauthorised installation of software, including personal software, on council-owned devices is prohibited.

6.3 Council networks and internet connections must be used responsibly and efficiently for authorised purposes.

6.4 Users should avoid excessive personal internet usage and activities that may compromise network security or performance.

7. Data Management and Security

7.1 All personal data processed by the Council must be handled in accordance with UK GDPR and the Data Protection Act 2018.

7.2 Personal data must be:

Processed lawfully and fairly

Protected from unauthorised access

Accessed only by authorised persons

Stored securely using approved systems and methods

7.3 Regular backups of council data must be undertaken to reduce the risk of data loss.

7.4 Secure data destruction methods must be used where appropriate.

7.5 Data must only be retained for as long as necessary and securely deleted when no longer required.

8. Monitoring of IT Systems and Email

8.1 Chilton Polden Parish Council reserves the right to monitor the use of council email systems, internet usage, and IT equipment to ensure compliance with this policy and relevant legislation.

8.2 Monitoring will be conducted in accordance with UK GDPR and the Data Protection Act 2018.

8.3 Monitoring shall be proportionate and limited to what is necessary to protect council systems and ensure lawful and appropriate use.

9. Retention and Archiving

9.1 Emails and electronic records must be retained and archived in accordance with legal, regulatory, and council record retention requirements.

9.2 Users should regularly review and securely delete unnecessary emails and files to maintain organised and efficient systems.

10. Security Incidents and Data Breaches

10.1 Any suspected cyber security incident, data breach, or loss of council data must be reported immediately to the Parish Clerk or designated IT contact.

10.2 The Council will respond to security incidents and data breaches in accordance with UK GDPR and the Data Protection Act 2018.

10.3 Where required, breaches will be reported to the Information Commissioner's Office (ICO).

11. Use of Mobile Devices and Remote Working

11.1 Council-owned mobile devices and IT equipment must be used only for authorised purposes.

11.2 Devices must be protected with:

Secure passwords or passcodes

Up-to-date antivirus protection

Firewall protection

Biometric authentication where available

11.3 When working remotely, users must follow the same security practices as when working from council premises.

11.4 Where personal devices are used for council business, users are encouraged to maintain appropriate security protections.

11.5 Sensitive council information should not be accessed on public Wi-Fi networks unless approved security measures are in place.

12. Software and System Security

12.1 All council IT equipment must have appropriate security protections including antivirus software and firewalls.

12.2 Security updates and software patches must be installed regularly.

12.3 Unapproved software or applications must not be installed on council-owned equipment.

13. Council Website and Social Media

13.1 The Council's website and social media platforms must be managed responsibly and in accordance with relevant legislation.

13.2 All published content must comply with:

UK GDPR

Data Protection Act 2018

Relevant NALC guidance

Copyright and defamation laws

13.3 Content published on behalf of the Council must be accurate, respectful, professional, and appropriate to the role of a public authority.

14. Training and Awareness

14.1 The Council will seek to ensure that councillors, employees, and authorised users are aware of their responsibilities regarding:

Data protection

Cyber security

Appropriate use of council IT systems

Email security and phishing awareness

14.2 Training and guidance may be provided where necessary to support compliance with this policy.

15. Compliance and Consequences

15.1 Failure to comply with this policy may result in:

Removal or suspension of access to council IT systems

Investigation by the Council

Further action considered appropriate by the Council

15.2 Serious breaches may also result in action under relevant legislation, including the Data Protection Act 2018.

16. Policy Review

16.1 This policy shall be reviewed annually by Chilton Polden Parish Council to ensure it remains compliant with legislation, cyber security guidance, and best practice.

16.2 The Council may amend this policy at any time to address emerging technology risks or operational requirements.

17. Contact

For IT-related enquiries, support, or to report security concerns, please contact:

Clerk / Responsible Officer: _____

Email: _____

Telephone: _____

All councillors, employees, volunteers, contractors, and authorised users share responsibility for protecting the security and integrity of the Council's IT systems and information.

By adhering to this policy, Chilton Polden Parish Council aims to maintain a secure, reliable, and efficient IT environment that supports effective local governance and communication.

Date Adopted: _____

Review Date: _____

Approved By: **R James** _____

Signature: _____

