MARCH 2026

IT POLICY
For Town and Parish Councils
Incorporating Assertion 10 Requirements
Practitioners' Guide 2025

Cholesbury-cum-St Leonards

Parish Council (CCSLPC)

NOTES:

1. Sections highlighted are not specifically relevant to CCSLPC at present, as it does not own any IT equipment. The draft text has been ~~struck through~~ but left in place in case the situation changes in the future.
2. Councillors' and employee's attention are drawn in particular to sections in red, which cover the use of Personal Devices and Emails.
3. The Council is aiming to achieve the Policy set out in Section 4.1 (relating to use of Email addresses) and anticipates achieving these objectives by May 2026. [The Policy has been achieved for the Clerk, the Chair, the Vice Chairs and the majority of Cllrs.]

1. INTRODUCTION AND PURPOSE

1.1 PURPOSE

This policy sets out the principles, procedures, and expectations for the use, management, and protection of information technology (IT) systems and data within Cholesbury-cum-St Leonards Parish Council.

The policy is designed to ensure compliance with Assertion 10 of the Annual Governance Statement (Section 1 of the Annual Governance and Accountability Return) and paragraph 1.54 of the Practitioners' Guide 2025, which states:

> *"All smaller authorities (excluding parish meetings) must also have an IT policy. This explains how everyone — clerks, members and other staff — should conduct authority business in a secure and legal way when using IT equipment and software. This relates to the use of authority-owned and personal equipment."*

1.2 SCOPE

This policy applies to:

- All councillors (members)
- The Clerk and any employees
- Contractors and volunteers
- Any third parties acting on behalf of the Council

The policy covers the use of:

- Council-owned IT equipment (computers, laptops, tablets, smartphones, printers)
- Personal devices used to access council data or systems (BYOD)
- Council-provided email accounts and communication services
- Internet access and online services
- Council website and social media accounts
- Software applications and cloud services
- Data storage systems and backups

1.3 DEFINITIONS

Users:

Councillors, employees, volunteers, contractors, and third parties acting on behalf of the Council.

Data:

Digitally stored information including documents, images, personal information, financial records, and correspondence.

IT Equipment/Hardware:

Includes but is not limited to computers, laptops, tablets, smartphones, printers, scanners, network equipment, and storage devices.

Software:

Operating systems, applications, email services, cloud platforms, and any digital tools used for Council business.

Personal Device (BYOD):

Any privately-owned device used to access Council data or conduct Council business.

2. IT SYSTEMS MANAGEMENT

2.1 COUNCIL-OWNED EQUIPMENT (CCSLPC HAS NONE)

~~All IT equipment and systems provided by the Council remain the property of the Council and shall be recorded on the asset register.~~

- ~~Equipment must be used primarily for Council business.~~
- ~~All devices must have up-to-date operating systems and security software installed.~~
- ~~Anti-virus and anti-malware software must be installed and kept current on all devices.~~
- ~~Automatic updates should be enabled where possible.~~
- ~~Equipment must not be modified, upgraded, or have unauthorised software installed without approval from the Clerk.~~
- ~~At the end of any period of office, employment, or engagement with the Council, all equipment must be returned to the Clerk in full working condition within 14 days.~~

2.2 SOFTWARE AND LICENSING (CCSLPC HAS NONE INSTALLED)

- ~~All software installed on Council devices must be legally licensed.~~
- ~~Only software approved by the Clerk may be installed on Council equipment.~~
- ~~Unlicensed or pirated software is strictly prohibited.~~
- ~~Software licences should be recorded and reviewed annually.~~

2.3 BACKUPS AND DATA RECOVERY

- Regular backups of all critical council data should be performed at least weekly.
- Backup copies must be stored securely, preferably in a separate location or using an encrypted cloud service.
- The Clerk shall ensure backup procedures are documented and tested periodically.
- A recovery plan should be in place to restore data in the event of loss or system failure.

2.4 ASSET MANAGEMENT

- An annual risk assessment should be undertaken regarding use and security of Council IT hardware, software, and stored data.

- A review of the Council's IT requirements should be conducted at least every four years, when council elections take place, or within three months of new staff starting.
- The Council maintains insurance on IT equipment; any loss or damage should be reported immediately to the Clerk.

3. USE OF PERSONAL DEVICES (BYOD)

3.1 PRINCIPLES

The Council recognises that councillors and staff may use their own personal devices to access Council data or conduct Council business. However, this introduces additional risks that must be managed.

The ICO has identified the use of personal devices and email addresses as one of the top data protection challenges for parish councils.

3.2 REQUIREMENTS FOR PERSONAL DEVICE USE

Where users access Council systems or data on personal devices, they must:

- Ensure the device is password/PIN protected or uses biometric authentication
- Keep the device's operating system and apps updated
- Have up-to-date anti-virus/security software installed
- Not allow other household members or third parties to access Council data
- Ensure Council data is not stored on the device longer than necessary
- Use only secure, encrypted connections when accessing Council data remotely
- Report immediately to the Clerk if the device is lost, stolen, or compromised
- Agree to remote wipe of Council data if the device is lost or stolen (where technically feasible)

3.3 LIMITATIONS

- Sensitive or confidential Council data should not be stored on personal devices unless necessary and only with appropriate encryption.
- Personal email accounts must not be used for Council business correspondence (see Section 4).
- The Council is not responsible for the maintenance, repair, or replacement of personal devices.

4. EMAIL AND COMMUNICATIONS

4.1 COUNCIL EMAIL ACCOUNTS

Official council email addresses (e.g., clerk@[council].gov.uk) must be used for all Council correspondence.

- An email address will be provided to all councillors and employees for official use.

- Personal email addresses (e.g., Gmail, Hotmail, Yahoo) must not be used for Council business.
- Council emails must not be forwarded to personal email accounts.
- Email accounts remain the property of the Council and may be accessed by authorised personnel.

4.2 EMAIL SECURITY

- Be vigilant for phishing emails and never click on suspicious links or attachments.
- Never share passwords or respond to requests for credentials via email.
- Report any suspicious emails to the Clerk immediately.
- Use strong, unique passwords for email accounts (see Section 6).
- Two-factor authentication must be enabled where available.

4.3 EMAIL RETENTION

- Emails should be retained in accordance with the Council's Document Retention Policy.
- Emails relating to Council business may be subject to disclosure under the Freedom of Information Act 2000 or Data Protection legislation.
- Regularly review and delete unnecessary emails to maintain security and compliance.

4.4 PROFESSIONAL STANDARDS

- All email communications must be professional, respectful, and appropriate.
- Council emails must not be used for personal purposes.
- Confidential information must be handled appropriately and marked clearly.

5. INTERNET AND ACCEPTABLE USE

5.1 INTERNET USE (NOT RELEVANT)

- ~~Council internet access is provided for official Council purposes.~~
- ~~Limited personal use may be permitted provided it does not interfere with work duties or compromise security.~~
- ~~Accessing illegal, inappropriate, or offensive content is strictly prohibited.~~
- ~~Downloading or streaming non-work content that consumes excessive bandwidth is not permitted.~~
- ~~Installing software from the internet without authorisation is prohibited.~~

5.2 PROHIBITED ACTIVITIES

Users must not:

- Access or distribute illegal, obscene, or offensive material
- Use Council IT for personal commercial activities
- Engage in any activity that could bring the Council into disrepute
- Attempt to circumvent security controls or access restricted systems
- Download or install pirated software, music, videos, or other copyrighted material

- ~~Use Council systems for gambling or illegal activities~~
- ~~Introduce malware, viruses, or other malicious code~~

5.3 NETWORK SECURITY

- Avoid using unsecured public Wi-Fi networks to access Council data.
- If remote working is necessary, use a secure VPN connection where available.
- Do not connect unknown USB devices or external storage to Council equipment.

6. PASSWORD AND ACCESS SECURITY

6.1 PASSWORD REQUIREMENTS

Strong passwords are essential for protecting Council systems and data.

- Passwords should be at least 12 characters long (ideally 20+ for sensitive systems).
- Use a combination of uppercase and lowercase letters, numbers, and special characters.
- Alternatively, use a passphrase of four or more random words joined with non-alphanumeric characters.
- Never use easily guessed information (names, birthdays, common words).
- Never reuse passwords across different systems or between personal and Council accounts.
- Never share passwords with anyone.
- Never write down passwords in visible locations.
- Change passwords immediately if a breach is suspected.

6.2 TWO-FACTOR AUTHENTICATION (2FA)

- Two-factor authentication must be enabled on all Council accounts where available.
- Preferred methods: authentication apps or hardware security keys.
- SMS-based 2FA is acceptable but less secure.

6.3 ACCESS CONTROL

- Access to Council systems and data is restricted to authorised users only.
- User accounts must be reviewed periodically and removed when no longer required.
- Users must not share login credentials or allow others to use their accounts.
- Devices must be locked when unattended (auto-lock should be enabled).
- Generic or shared accounts should be avoided where possible.

7. DATA PROTECTION AND CONFIDENTIALITY

7.1 LEGAL REQUIREMENTS

All personal and sensitive data must be handled in accordance with:

- UK General Data Protection Regulation (UK GDPR)

- Data Protection Act 2018
- Freedom of Information Act 2000
- Environmental Information Regulations 2004

7.2 DATA HANDLING

- Personal data should only be accessed by those who require it for their work.
- Data must be stored securely with appropriate access controls.
- Personal data must not be stored longer than necessary (see Retention Policy).
- Electronic records must be protected from unauthorised access, disclosure, alteration, and destruction.
- Sensitive data must not be stored unencrypted on USB sticks, personal laptops, or unapproved cloud services.

7.3 DATA TRANSFER

- Personal data should only be shared where there is a lawful basis to do so.
- When emailing sensitive information, consider using encryption or password-protected attachments.
- Do not use unapproved file-sharing services for Council data.

7.4 SUBJECT ACCESS REQUESTS AND FOI

Users should be aware that any Council correspondence, including emails (even on personal accounts if used for Council business), may be subject to disclosure under data protection or freedom of information legislation.

8. SOCIAL MEDIA

8.1 OFFICIAL COUNCIL SOCIAL MEDIA

- Only designated personnel may post on official Council social media accounts.
- All posts should be professional, accurate, and reflect the Council's position.
- Content should be reviewed for accuracy before posting.
- Comments and messages should be monitored and responded to appropriately.
- The Clerk should approve the creation of any new social media accounts.

8.2 PERSONAL USE OF SOCIAL MEDIA

- When using social media in a personal capacity, users must make it clear they are not representing the Council.
- Users must follow the Council's Code of Conduct when discussing Council matters online.
- Confidential Council information must never be shared on social media.
- Users should be mindful that personal posts could reflect on the Council.

9. WEBSITE MANAGEMENT

The Council website must:

- Be kept accurate and up-to-date with current information
- Meet WCAG 2.2 AA accessibility standards
- Publish all documents required by the Transparency Code
- Include appropriate privacy notices and cookie policies
- Be regularly reviewed for security vulnerabilities
- Be hosted on a secure, reputable platform
- Have regular backups maintained

10. ARTIFICIAL INTELLIGENCE (AI)

10.1 PRINCIPLES FOR AI USE

The Council recognises that AI tools (such as ChatGPT, Microsoft Copilot, and similar) may offer productivity benefits but also present risks that must be managed.

- AI may be used as a productivity tool to assist with drafting, research, and administrative tasks.
- AI output must always be reviewed by a human for accuracy before use.
- Users must understand that AI can generate inaccurate or biased information.

10.2 DATA PROTECTION AND AI

- Personal, confidential, or sensitive Council data must not be entered into public AI tools (e.g., free versions of ChatGPT).
- Any use of AI that processes personal data may require a Data Protection Impact Assessment.
- Users must check the data handling and privacy policies of any AI tool before use.

10.3 TRANSPARENCY

- Documents substantially created using AI should be disclosed as such.
- AI-generated content should not be presented as original human work without review and editing.

10.4 COPYRIGHT AND ACCURACY

- AI must not be used to generate content that infringes intellectual property rights.
- AI output should be fact-checked and verified before reliance or publication.
- Users remain responsible for any content they produce, regardless of AI assistance.

11. INCIDENT REPORTING AND BREACH RESPONSE

11.1 REPORTING REQUIREMENTS

Any incidents that may compromise Council data or systems must be reported to the Clerk immediately. This includes:

- Lost or stolen devices (Council-owned or personal devices with Council data)
- Suspected data breaches or unauthorised access
- Phishing attempts or suspicious communications
- Shared or compromised passwords
- Malware or virus infections
- Any suspicious activity on Council systems

11.2 BREACH RESPONSE

- All incidents will be logged and investigated.
- Personal data breaches must be assessed against GDPR notification requirements (report to ICO within 72 hours if required).
- Affected individuals will be notified where necessary.
- Remedial actions will be taken to prevent recurrence.

11.3 CRIMINAL ACTIVITY

Any criminal damage, theft, or suspected criminal activity will be reported to the Police.

12. MONITORING AND COMPLIANCE

12.1 MONITORING

The Council reserves the right to monitor the use of its IT resources to ensure compliance with this policy and legal requirements. This may include:

- Reviewing email and internet usage logs
- Auditing access to systems and data
- Monitoring for security threats

Monitoring will be conducted in accordance with data protection legislation and any applicable employment law requirements.

12.2 COMPLIANCE

All users are required to comply with this policy. Breach of this policy may result in:

- Suspension of IT privileges
- Disciplinary action (for employees)
- Referral to external authorities where appropriate
- Potential legal action in serious cases

13. TRAINING AND AWARENESS

- All users will be made aware of this policy and their responsibilities.
- Training on IT security, data protection, and phishing awareness will be provided as appropriate.
- New councillors and employees will receive IT induction training.
- Refresher training will be provided annually or when significant changes occur.

14. REVIEW AND UPDATES

- This policy will be reviewed annually, or sooner if required by changes in legislation, Council operations, technology, or best practice guidance.
- Updates will be communicated to all relevant parties.
- The Clerk is responsible for maintaining this policy and ensuring it remains current.

15. RESPONSIBILITIES

THE CLERK (OR DESIGNATED IT OFFICER):

- Implementing and overseeing this policy
- Managing IT assets and maintaining the asset register
- Ensuring backups are performed and tested
- Managing user accounts and access
- Responding to IT incidents and breaches
- Arranging training and awareness activities
- Keeping this policy under review

ALL USERS:

- Adhering to this policy at all times
- Protecting Council data and IT resources
- Using strong passwords and security measures
- Reporting incidents and concerns promptly
- Completing required training
- Seeking guidance if uncertain about any aspect of this policy

16. RELATED POLICIES

This policy should be read in conjunction with:

- Data Protection Policy
- Privacy Notice
- Code of Conduct
- Standing Orders and Financial Regulations
- Risk Management Policy