BOXTED PARISH COUNCIL

INFORMATION TECHNOLOGY (IT) POLICY

Adopted	14 Oct 2026
Minute reference	26/165
Review date	Oct 2027

Contents

1. Purpose 2
2. Scope 2
3. Council IT equipment 2
4. CloudyIT 3
5. Council email 3
6. Passwords and authentication 3
7. Cloud storage and Council records 4
8. Personal devices 4
9. Cyber security 4
10. Suspected security incidents 5
11. Backup and recovery 5
12. Use of the Council laptop 5
13. Software and downloads 6
14. Confidential and sensitive information 6
15. Freedom of Information and transparency 6
16. Social media and public communications 6
17. Use of artificial intelligence (AI) 7
18. Council website 7
19. Remote working 8
20. Physical security of the Council laptop 8
21. Changes to users and access 8
22. Training and awareness 8
23. Responsibilities 9
24. Monitoring and audit 9
25. Breaches of this policy 9
26. Review 9
Appendix A – Current Council IT Arrangements 10
Appendix B – Basic Security Rules for All Users 10

1. Purpose

Boxted Parish Council recognises that secure and reliable information technology is essential to the effective administration of the Council.

This policy sets out how the Council's information technology, electronic communications and digital information are to be used securely, responsibly and lawfully.

This policy aims to:

- protect Council information and personal data;
- reduce the risk of loss, theft, malware, phishing, ransomware and unauthorised access;
- ensure that Council IT equipment is used appropriately;
- establish clear responsibilities for councillors, the Clerk and other authorised users;
- support compliance with the UK GDPR, the Data Protection Act 2018 and other relevant legislation; and
- assist the Council in meeting the requirements relating to IT and cyber security under the Practitioners' Guide and Assertion 10 of the Annual Governance and Accountability Return (AGAR).

2. Scope

This policy applies to all Parish Councillors; the Clerk and any other Council employees; and contractors, volunteers or other people authorised to access Council IT systems or information.

It applies to the Council's laptop, email accounts, Microsoft 365 services, cloud storage, Council website and any other IT systems or services provided or authorised by the Council.

3. Council IT equipment

The Council currently operates with one Council-owned laptop, principally used by the Clerk for Council business.

The laptop remains the property of the Parish Council and must not be used by unauthorised people.

The laptop should:

- be protected by a secure password/PIN;
- have the security and software updates provided or managed through the Council's IT support arrangements;
- have appropriate anti-malware and endpoint protection;
- be locked whenever it is left unattended;
- be physically secured when appropriate;
- not be lent to family members, friends or other unauthorised people; and
- only have software installed where this is authorised and appropriate for Council business.

The Council will not normally store Council records on local personal computers or other privately owned devices.

4. CloudyIT

The Council has appointed CloudyIT as its IT support and security provider.

CloudyIT will provide such IT management, security, maintenance, support, monitoring, backup and other services as are included within the Council's current contract.

The Clerk will act as the Council's principal contact with CloudyIT unless the Council decides otherwise.

The Council will rely upon CloudyIT's professional advice concerning the technical security and configuration of the Council's IT systems, but the Council remains responsible for ensuring that appropriate governance arrangements are in place.

The Clerk must report significant IT problems, suspected security incidents or concerns about the Council's IT security to CloudyIT promptly.

The Council will review its CloudyIT arrangements periodically to ensure that the services provided remain appropriate to the Council's needs.

5. Council email

Council business should be conducted using the Council's authorised email accounts, which are issued to all relevant individuals. Councillors and officers should not normally use personal email accounts for Council business. Council email accounts must not be shared between users.

Users must take care when opening attachments or clicking links received by email. Unexpected requests for passwords, payments, bank details, confidential information or changes to payment arrangements must be treated with caution.

Where a request appears unusual or suspicious, the recipient should verify the request by another appropriate method before taking action.

6. Passwords and authentication

Passwords and authentication credentials are personal to the authorised user and must not be disclosed to another person.

Passwords should:

- be difficult for others to guess;
- not be reused for unrelated personal services where this can reasonably be avoided;
- not be written where they can be readily accessed by unauthorised people; and
- be changed or reset where there is reason to believe that they may have been compromised.

Where multi-factor authentication (MFA) is available and supported by the Council's IT arrangements, it should be enabled in accordance with CloudyIT's recommendations.

Users must never approve an unexpected MFA request. Where the Council uses a password-management system supplied or recommended by CloudyIT, users must follow the security requirements of that system.

7. Cloud storage and Council records

Council documents and records should be stored only in Council-approved locations.

Where the Council uses Microsoft 365, OneDrive, SharePoint or another CloudyIT-supported cloud service, Council information should be stored within the Council's authorised account rather than a personal cloud-storage account.

Council documents must not be routinely stored in personal Google Drive, iCloud, Dropbox, OneDrive, USB storage or other personal cloud or storage accounts.

The Council's electronic records remain Council records and must be managed in accordance with the Council's document retention and data protection arrangements.

8. Personal devices

The Clerk and Councillors may need to use personal phones, tablets or computers to access Council email or documents. Where personal devices are used for Council business, users must take reasonable steps to protect Council information.

Personal devices used for council business should:

- be protected by a password, PIN or biometric security;
- use current operating-system and security updates;
- have appropriate screen locking enabled;
- not be shared with other people while Council information is accessible; and
- not be used to store Council information unnecessarily.

Council information should not normally be copied to personal devices where it can reasonably be accessed through the Council's approved cloud systems.

The Council does not require access to a councillor's personal device for routine monitoring or inspection. If a Council data breach is suspected, the Council may seek appropriate technical or legal advice concerning information held on a personal device.

9. Cyber security

All users must take reasonable precautions against cyber threats, including phishing, malware, ransomware, fraudulent emails, unauthorised access, identity theft and social engineering.

Users must not deliberately disable or circumvent security controls installed or managed by the Council or CloudyIT. Users must not install unauthorised software intended to bypass Council security controls.

The Council will consider cyber-security advice provided by CloudyIT and implement reasonable recommendations appropriate to the Council's size, resources and level of risk.

10. Suspected security incidents

A suspected security incident must be reported as soon as possible to the Clerk and, where appropriate, CloudyIT.

Examples of suspected security incidents include:

- a lost or stolen Council laptop;
- a lost or stolen phone containing Council information;
- a suspected phishing attack;
- clicking on a suspicious link or attachment;
- disclosure of a password;
- an unexpected MFA request being approved;
- suspected malware or ransomware;
- sending personal or confidential information to the wrong person; or
- unauthorised access to a Council account or document.

Users should not attempt to conceal an incident because they are concerned that they may have made a mistake. Prompt reporting enables the Council and CloudyIT to take appropriate action.

Where an incident involves personal data, the Clerk will consider whether it constitutes a personal data breach and whether it needs to be recorded or reported under the Council's data protection procedures (a notifiable breach must be reported to the ICO within 72 hours of the council becoming aware of it).

11. Backup and recovery

Council electronic records must be protected against accidental deletion, equipment failure, cyber attack and other forms of data loss.

The Council will use the backup arrangements included within its CloudyIT contract and/or authorised Microsoft 365 services. When reviewing and renewing this contract the council should consider suitability of the backup arrangements provided.

The Clerk will liaise with CloudyIT concerning the operation of backups; retention arrangements; recovery of accidentally deleted or corrupted information; and testing or verification of backup and recovery arrangements where appropriate.

The Council will not rely solely upon the Council laptop as the permanent storage location for important Council records.

12. Use of the Council laptop

The Council laptop is primarily provided for Council business.

Reasonable and limited personal use may be permitted by the Clerk where such use does not interfere with Council duties, incur significant cost to the Council, compromise Council security, involve inappropriate or unlawful material, or breach any Council policy.

The laptop must not be used for activities that could reasonably expose the Council to malware, legal liability, reputational damage or unacceptable security risk.

13. Software and downloads

Users must not install software on the Council laptop unless authorised by the Clerk and, where appropriate, CloudyIT.

Software, browser extensions and applications obtained from unknown or untrusted sources must not be installed.

Users should not download Council documents to personal devices unless there is a legitimate Council purpose and appropriate security arrangements are in place. These documents should be permanently deleted as soon as no longer required.

14. Confidential and sensitive information

Council information must be handled according to its sensitivity. Particular care must be taken with personal data; employee information; financial information; bank details; complaints and correspondence containing personal information; information relating to vulnerable individuals; and information that is confidential for legal or other legitimate reasons.

Before sending sensitive information electronically, the sender must check the recipient and ensure that the method of transmission is appropriate.

Where an email contains confidential or sensitive information, the sender should clearly identify this where appropriate.

15. Freedom of Information and transparency

The use of electronic systems does not alter the Council's legal obligations concerning Freedom of Information, Environmental Information, data protection or the retention of Council records.

Users must not delete, alter or conceal Council records in order to prevent or frustrate a legitimate information request.

The Clerk will manage information requests in accordance with the Council's adopted procedures.

16. Social media and public communications

Only people authorised by the Council may publish information on behalf of the Council through official Council social-media accounts or other official digital channels.

Councillors remain responsible for ensuring that their personal use of social media does not improperly represent their personal views as those of the Council.

Council IT systems must not be used to make discriminatory, offensive, defamatory, threatening or otherwise unlawful communications.

17. Use of artificial intelligence (AI)

The Council does not wish to restrict the sensible use of artificial intelligence (AI) tools, such as AI chatbots, writing assistants, summarising and transcription tools, and AI features built into software like Microsoft 365, where they help the Council work more efficiently. This section sets out a few ground rules so that AI is used safely and openly.

Users must not enter personal data, or confidential Council information, into an AI tool unless the Council has approved that tool for the purpose (taking advice from CloudyIT where appropriate). Personal data includes names, addresses, contact details and employee or financial information relating to an identifiable person.

Free or publicly available AI tools may keep what is entered into them and use it to develop their services, so anything entered should be treated as if it were being published. Where AI would be helpful, users should remove or anonymise personal details first (for example, by referring to "Resident A"), unless these are from a publicly available document (for example online planning application).

AI can produce inaccurate, out-of-date or misleading content. Users remain responsible for checking anything produced with the help of AI before relying on it, sending it or presenting it to the Council. AI should not be the sole basis for a Council decision.

Where AI has been used to help prepare a report, draft policy, response or other paper put to the Council or a committee for discussion or approval, the person presenting it should say so (for example, in a short note on the paper or when introducing the item), so that councilors can take that into account. This does not apply to routine tools such as spell-check, grammar suggestions or formatting. The author remains responsible for the content.

AI note-taking, recording or transcription tools should only be used in Council or committee meetings where the Council has agreed and attendees have been told. The Clerk remains responsible for the accuracy of the minutes, which continue to be approved by the Council in the usual way.

If personal data or confidential information is entered into an AI tool in breach of this section, it should be reported as a suspected security incident under section 10.

18. Council website

The Council website is an official Council communication channel. Responsibility for administration and publication on the website will rest with the persons authorised by the Council.

Website access credentials must be kept secure and must not be shared unnecessarily.

Where website services are provided by an external supplier, access should be restricted to authorised users and managed in accordance with the supplier's security arrangements.

19. Remote working

The Clerk may undertake Council work remotely using the Council laptop and authorised cloud services.

When working away from home or the Council's normal location, reasonable precautions must be taken to prevent unauthorised persons from viewing Council information.

The Council laptop should not be left unattended in a vehicle. Where working in public places, users should take particular care when displaying confidential information on screen.

Public Wi-Fi should only be used where appropriate security measures are in place and in accordance with CloudyIT's advice.

20. Physical security of the Council laptop

The Council laptop should be kept in a secure location when not in use.

If the laptop is lost or stolen, the Clerk must report the incident immediately to CloudyIT and the Council Chairman, or another nominated councillor if the Chairman is unavailable.

CloudyIT should be asked to take any appropriate action available to protect Council accounts and information, including remote security measures where supported by the Council's IT configuration.

21. Changes to users and access

When a Clerk, councillor, employee or other authorised user ceases to require access to Council IT systems, the Clerk or Chairman must ensure that appropriate steps are taken promptly.

These steps may include:

- disabling or removing access;
- changing passwords or access credentials;
- recovering Council equipment;
- transferring Council records;
- removing access to shared documents; and
- notifying CloudyIT.

The Council should retain access to Council records independently of an individual councillor's personal account or device.

22. Training and awareness

The Council will make appropriate information or training available to users concerning secure use of Council IT; phishing and other cyber threats; data protection; password and MFA security; reporting security incidents; and the appropriate use of Council email and cloud services.

The Council will consider training or security awareness advice provided by CloudyIT.

23. Responsibilities

The Parish Council is responsible for approving this policy and ensuring that appropriate resources are made available for the secure operation of its IT systems.

The Clerk is responsible for day-to-day administration of Council IT; liaison with CloudyIT; managing authorised access; reporting significant incidents; ensuring Council records are appropriately managed; and bringing significant IT risks to the Council's attention.

Councillors and other users are responsible for complying with this policy; protecting Council information; keeping passwords and authentication details secure; taking reasonable precautions against cyber threats; and reporting suspected security incidents promptly.

CloudyIT is responsible for delivering the technical support, security, maintenance, monitoring and other services specified in the Council's current contract. The Council will refer technical matters to CloudyIT rather than attempting to make unauthorised changes to managed security systems.

24. Monitoring and audit

The Council recognises that appropriate monitoring of its IT systems may be necessary to maintain security, investigate incidents and demonstrate compliance.

Where monitoring is undertaken by CloudyIT, it will be carried out in accordance with the Council's contract, applicable law and CloudyIT's service arrangements.

The Council will not routinely monitor users' personal devices.

25. Breaches of this policy

Failure to comply with this policy may expose the Council, its councillors, employees or others to security, financial, legal or reputational risks.

Where an employee breaches this policy, the matter may be dealt with under the Council's employment and disciplinary procedures where appropriate.

Where a councillor or other user breaches the policy, the Council may restrict or withdraw access to Council IT systems where this is necessary to protect Council information. Consideration will also be made as to whether the breach is notifiable to the Monitoring Officer.

Serious incidents may also need to be reported to the ICO, police, insurers, CloudyIT or other appropriate bodies.

26. Review

This policy will be reviewed at least annually and sooner if there is a significant change to the Council's IT systems; a change to the CloudyIT contract or security arrangements; a significant cyber-security incident; a relevant change in legislation or official guidance; or a material change in the Council's working arrangements.

Appendix A – Current Council IT Arrangements

Complete or amend this table to reflect the Council's actual CloudyIT contract and systems.

Area	Council arrangement
Council-owned computers	One laptop
IT support/security	CloudyIT
Email	Council-authorised email system
Cloud services	Microsoft 365 / services authorised by the Council
Council document storage	Council-authorised cloud storage
Backup	CloudyIT / contracted cloud backup arrangements
Personal devices	Permitted for limited Council access subject to this policy
Main IT user	Clerk
IT support contact	01280 830025
IT/security incidents	Clerk and CloudyIT
Policy owner	Parish Council

Appendix B – Basic Security Rules for All Users

1. Never share your password.
2. Never approve an unexpected MFA request.
3. Treat unexpected emails and attachments with caution.
4. Check payment and bank-detail changes independently.
5. Keep devices locked when unattended.
6. Keep software and operating systems up to date.
7. Do not store Council files in personal cloud accounts.
8. Do not install unauthorised software.
9. Report lost devices or suspected cyber incidents immediately.
10. If in doubt, contact the Clerk or CloudyIT before taking action.