BREDHURST PARISH COUNCIL

Cyber Security Policy

Version: 3.0
Adopted: October 2024
Reviewed: November 2026
Next Review: November 2027

1. Purpose

recognises the importance of protecting its information, systems, equipment, and data from cyber threats. The Council is committed to maintaining appropriate security measures to safeguard personal data, financial information, council records and digital services.
This policy establishes the standards and responsibilities for cyber security and applies to all councillors, employees, contractors, volunteers, and anyone authorised to access council information or systems.
The Council will take reasonable and proportionate steps to protect its information assets against unauthorised access, loss, theft, disclosure, corruption, cyber-attack, or misuse.

2. Scope

This policy applies to:

- Council-owned devices and equipment.
- Personal devices used to access council information.
- Council email accounts.
- Microsoft 365, OneDrive, SharePoint and other approved cloud services.
- Council websites and social media accounts.
- Electronic records and digital communications.
- Contractors and third parties who process council information on behalf of the Council.

3. Responsibilities

The Council
The Council is responsible for:

- Establishing appropriate cyber security arrangements.
- Providing suitable equipment and software where required.
- Ensuring compliance with data protection legislation.
- Maintaining appropriate backup and recovery procedures.
- Reviewing this policy annually.

The Clerk
The Clerk is responsible for:

- Day-to-day administration of council information and systems.
- Reporting cyber incidents promptly.
- Ensuring software and security updates are applied.
- Maintaining records of cyber incidents and security breaches.
- Liaising with the Council's IT support provider where necessary.

Councillors, Staff and Other Users
All users must:

- Comply with this policy.
- Take reasonable care of council information.

- Report suspected cyber incidents without delay.
- Follow good cyber security practices at all times.

4. Access Control

Access to council systems shall be restricted to authorised users only.
Users must:

- Use only authorised accounts to access council information.
- Keep login credentials confidential.
- Log out of systems when no longer required.
- Lock devices whenever left unattended.
- Ensure appropriate permissions are granted only to those who require access.

Access shall be removed promptly when a councillor, employee, volunteer or contractor no longer requires it.

5. Passwords and Authentication

Strong authentication is one of the Council's primary cyber security controls.
Users must:

- Use strong, unique passwords or passphrases with a minimum of 12 characters wherever systems permit.
- Avoid using easily guessed information such as names, birthdays or common words.
- Never share passwords unless authorised and absolutely necessary.
- Enable Multi-Factor Authentication (MFA) on all accounts where available.
- Avoid reusing passwords across different systems.

Password managers may be used to securely store and generate passwords.
Passwords should be changed immediately if there is reason to believe an account has been compromised.

6. Use of Council and Personal Devices

Where council information is accessed using either council-owned or personal devices, users must ensure:

- Devices are protected by passwords, PINs or biometric security.
- Operating systems and software remain fully updated.
- Anti-virus and malware protection is installed and maintained where appropriate.
- Device encryption is enabled whenever available.
- Devices are not left unattended in public places.
- Council information is removed from personal devices when it is no longer required.

Users should avoid accessing council information from shared or public computers.

7. Email and Phishing Protection

Email remains one of the most common routes for cyber-attacks.
Users must:

- Treat unexpected emails with caution.
- Verify unusual requests before responding.
- Avoid opening suspicious attachments.
- Avoid clicking links that appear suspicious or unexpected.
- Check sender addresses carefully.
- Report suspected phishing attempts immediately.

Particular care should be taken when receiving requests relating to payments, bank details, invoices or personal information.

8. Microsoft 365 and Cloud Services

Council information must only be stored in approved locations.
Users must:

- Store council records within approved Microsoft 365 services or other authorised systems.
- Avoid using personal cloud storage accounts for council business.
- Ensure files containing personal or sensitive information are shared only with authorised recipients.
- Apply appropriate permissions and access restrictions to shared documents.

Council information must not be transferred to unauthorised third-party platforms.

9. Secure Data Handling

Users handling personal or confidential information must:

- Comply with UK GDPR and the Data Protection Act 2018.
- Access only information required for their role.
- Share information only where there is a legitimate council purpose.
- Use secure methods when transferring sensitive information.
- Ensure recipients are authorised to receive information.

Care should be taken to minimise the amount of personal data shared or stored.

10. Software and Updates

To reduce cyber security risks:

- Security updates should be installed as soon as reasonably practicable.
- Unsupported software must not be used for council business.
- Users must not install unauthorised software on council equipment.
- Software should only be obtained from legitimate and trusted sources.

11. Backups and Recovery

Appropriate arrangements shall be maintained to protect council records against accidental loss, technical failure or cyber-attack.
Where applicable:

- Council data should be backed up through approved systems.
- Backups should be protected from unauthorised access.
- Recovery arrangements should be tested periodically.

12. Cyber Incident and Data Breach Reporting

Any actual or suspected cyber security incident must be reported immediately to the Clerk and Chair of the Council.
Examples include:

- Phishing attacks.
- Malware infections.
- Unauthorised access to systems.
- Loss or theft of equipment.
- Misdirected emails containing personal data.
- Suspected data breaches.

Users should report incidents as soon as possible and, wherever practicable, within 24 hours of discovery.
The Council will investigate incidents and, where required, consider notification obligations under UK GDPR and other relevant legislation.

13. Remote Working

Where council business is conducted remotely, users must:

- Use secure internet connections.
- Keep devices physically secure.
- Prevent unauthorised persons from viewing confidential information.
- Follow the requirements of this policy at all times.

Public Wi-Fi should be avoided when accessing sensitive council information unless an appropriate secure connection is used.

14. Social Media and Internet Use

Users must:

- Use council accounts responsibly.
- Avoid posting confidential or personal information.
- Exercise caution when following links from online sources.
- Comply with the Council's Social Media Policy and other relevant policies.

15. Training and Awareness

The Council encourages councillors and staff to remain aware of emerging cyber threats and good security practices.
Cyber security awareness guidance and training may be provided periodically to support compliance with this policy.

16. Monitoring and Compliance

The Council reserves the right to investigate any suspected breach of this policy and take appropriate action.
Failure to comply may result in:

- Informal or formal action in accordance with employment procedures.
- Referral to relevant councillor conduct arrangements.
- Termination of contractor or supplier agreements.
- Reporting to relevant authorities where appropriate.

Each incident will be considered on its own circumstances.

17. Review

This policy will be reviewed annually, or sooner if required by changes in legislation, guidance, technology or operational requirements.

Document Control

Version	Date	Description of Change	Approved By
1.0	October 2024	Original Policy	Full Council

2.0	October 2025	No Amendments	Full Council
3.0	November 2026	Comprehensive review and modernisation of cyber security controls	Full Council