BREDHURST PARISH COUNCIL

Cyber Security Policy

Adopted: October 2024

Introduction

Bredhurst Parish Council's cyber security policy outlines the guidelines and provisions for preserving the security of our data and technology infrastructure.

The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize Bredhurst Parish Council's reputation.

For this reason, a number of security measures have been implemented. Instructions have been prepared to help mitigate security risks and these are outlined in this policy.

This policy applies to the Clerk, Councillors, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware.

Confidential data

Confidential data is secret and valuable. Common examples are:

- Unpublished financial information
- Data of residents/hirers/contractors
- Customer lists (existing and prospective)

The Clerk and Councillors are obliged to protect this data. In this policy, instructions will be given on how to avoid security breaches.

Protect personal and company devices

When the Clerk or Councillors use their digital devices to access company emails or accounts, they introduce security risk to our data. We advise the Clerk and Councillors to keep both their personal and company-issued computer, tablet and cell phone secure. They can do this if they:

- Keep all devices password protected.
- Choose and upgrade a complete antivirus software.
- Ensure they do not leave their devices exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into company accounts and systems through secure and private networks only.
- We also advise the Clerk and Councillors to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

Keep emails safe

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct The Clerk and Councillors to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. “watch this video, it’s amazing.”)
- Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or giveaways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If the Clerk isn’t sure that an email, they have received is safe, he/she can refer to the Chair or Vice Chair.

Manage passwords properly

Password leaks are dangerous since they can compromise Bredhurst Parish Council’s entire infrastructure. Not only should passwords be secure so they won’t be easily hacked, but they should also remain secret. For this reason, Bredhurst Parish Council advises The Clerk and Councillors to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.)
- Remember passwords instead of writing them down. If The Clerk and Councillors need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Exchange credentials only when absolutely necessary. When exchanging them in-person isn’t possible, The Clerk and Councillors should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- The Clerk should change the password on the Parish Laptop every two months.
- Update the password folder and change this password every two months.

Transfer data securely

Transferring data introduces security risk. The Clerk and Councillors must:

- Avoid transferring sensitive data (e.g. customer information, employee records, financial records) to other devices or accounts unless absolutely necessary.
- Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies.
- Report scams, privacy breaches and hacking attempts to the Chair and Vice Chair.

Bredhurst Parish Council needs to know about scams, breaches and malware so it can better protect its infrastructure. For this reason, BPC advises The Clerk and Councillors to report perceived attacks, suspicious emails or phishing attempts as soon as possible to the Chair and Vice Chair. So that Bredhurst Parish Council can investigate promptly, resolve the issue and send an alert when necessary.

Additional measures

To reduce the likelihood of security breaches, The Parish Council also instruct its The Clerk and Councillors to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to the Chair and Vice Chair.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in the Parish Council laptop.
- Refrain from downloading suspicious, unauthorized or illegal software on the Parish Council laptop.
- Avoid accessing suspicious websites.

Bredhurst Parish Council also expects the Clerk and Councillors to comply with our social media and internet usage policy.

Disciplinary Action

Bredhurst Parish Council expects the Clerk and Councillors to always follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: We may issue a verbal warning and train the employee on security.
- Intentional, repeated or large-scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary action up to and including termination.
- We will examine each incident on a case-by-case basis.

Additionally, those who are observed to disregard Bredhurst Parish Council's security instructions will face progressive discipline, even if their behavior hasn't resulted in a security breach.

Take security seriously

Everyone, from Bredhurst Parish Council customers, residents, hirers of Blacksmith Barn and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.