CYBER SECURITY POLICY REVIEWED MAY 2025

Policy brief & purpose

Snodland Town Council cyber security policy outlines our 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 jeopardise Snodland Town Councils' reputation.

For this reason, we have implemented several security measures. We have also prepared instructions that may help mitigate security risks. Snodland Town Council have outlined both provisions in this policy.

Scope

This policy applies to all our users, councillors, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware. Throughout this policy they will be referred to as "users"

Policy Elements

Confidential data is secret and valuable. Common examples are:

- Unpublished financial information
- Data of customers/partners/vendors
- Patents, formulas or new technologies
- Customer lists (existing and prospective)

All users are obliged to protect this data. In this policy, Snodland Town Council will give users instructions on how to avoid security breaches.

Protect personal and council devices

When users use their digital devices to access council emails or accounts, they introduce security risk to our data. Snodland Town Council advise users to keep both their personal and any council-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 council accounts and systems through secure and private networks only.
- We also advise our users 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, Snodland Town Council instruct users 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 give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)
- If a user isn't sure that an email they received is safe, they can refer to the CEO.
- Adhere to the email policy

Manage passwords properly

Password leaks are dangerous since they can compromise Snodland Town Council entire infrastructure. Not only should passwords be secure, so they won't be easily hacked, but they should also remain secret. For this reason, Snodland Town Council advise users 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 users 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, users should prefer the phone instead of email, and only if they personally recognize the person they are talking to.

Transfer data securely

Transferring data introduces security risk.

users must:

- Avoid transferring sensitive data (e.g. customer information, user records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, Snodland Town Council request users to ask for help.
- Share confidential data over the council network/ system and not over public Wi-Fi or private connection.
- 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

Snodland Town Council need to know about scams, breaches, and malware so Snodland Town Council can better protect the infrastructure.

For this reason, we advise our users to report perceived attacks, suspicious emails, or phishing attempts as soon as possible to the CEO so that Snodland Town Council can investigate promptly, resolve the issue and send an alert when necessary.

Additional measures

To reduce the likelihood of security breaches, Snodland Town Council also instruct users to:

- lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in council systems.
- Refrain from downloading suspicious, unauthorised, or illegal software on council equipment.
- Avoid accessing suspicious websites.

Snodland Town Council also expect our users to comply with our social media and internet usage policy.

Snodland Town Council should:

- Install firewalls, anti-malware software and access authentication systems.
- Arrange for security training to all users.
- Inform users regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.

Remote users

Remote users must follow this policy's instructions too. Since they will be accessing Snodland Town Council systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

Snodland Town Council encourage them to seek advice from the CEO.

Disciplinary Action

Snodland Town Council expect all users to always follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: Snodland Town Council may issue a verbal warning and train the user on security.
- Intentional, repeated, or large-scale breaches (which cause severe 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, users who are observed to disregard Snodland Town Council security instructions will face progressive discipline, even if their behaviour hasn't resulted in a security breach.

Take security seriously

Everyone, from Snodland Town Council customers and partners to our users and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect Snodland Town Council systems and databases. Snodland Town Council can all contribute to this by being vigilant and keeping cyber security top of mind.