CYBER SECURITY POLICY

Introduction

SNAPS' 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 SNAPS' reputation.

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

Scope

This policy applies to all our employees, contractors, volunteers, Trustees and anyone who has permanent or temporary access to our systems and hardware.

Confidential Data

Confidential data is secret and valuable. Examples may be:

Unpublished financial information
Data regarding SNAPS' families
Data concerning SNAPS' staff, volunteers, Trustees or contractors
Data regarding SNAPS' supporters

All employees, volunteers, Trustees and contractors are obliged to protect this data. In this policy, we provide instructions on how to avoid security breaches.

Protect Personal and The Charity's Devices

When employees, volunteers, contractors and Trustees use their digital devices to access SNAPS' emails or accounts, they introduce security risks to SNAPS' data. Employees are advised to keep both their personal and SNAPS-issued computers, tablets and mobile phones 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 SNAPS' accounts and systems through secure and private networks only.

SNAPS' employees, volunteers, contractors and Trustees are encouraged to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

Emails

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct SNAPS' employees, volunteers, contractors and Trustees to:

Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing."), particularly from an unknown or unusual source,

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 SNAPS employee, volunteer, contractor or Trustee isn't sure that an email they have received is safe, they can refer to our Afinite, SNAPS' IT support.

Passwords

Password leaks are dangerous since they can compromise SNAPS' entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, we advise SNAPS' employees, volunteers, contractors and Trustees 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 employees 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, employees should prefer the phone instead of email, and only if they personally recognise the person they are talking to.

Transfer Data Securely

Transferring data introduces security risk. SNAPS' employees, volunteers, contractors and Trustees must:

Avoid transferring sensitive data (e.g. family information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees to ask our Afinite for help.

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.

Our IT advisers, Afinite, need to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise SNAPS' employees, volunteers, contractors and Trustees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our specialists.

Additional Measures

To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks;
- Report stolen or damaged equipment as soon as possible to your line manager,
- Change all account passwords at once when a device is stolen,
- Report a perceived threat or possible security weakness in SNAPS' systems,
- Refrain from downloading suspicious, unauthorised or illegal software on their SNAPS' equipment,
- Avoid accessing suspicious websites. We also expect SNAPS' employees, volunteers, contractors and Trustees to comply with our social media and internet usage policy,

- All SNAPS' devices should have firewalls, anti malware software and access authentication systems.

Process if Security Breach is Discovered

If a security breach is discovered, SNAPS Chief Executive should be informed immediately. They will assess the issue and take appropriate action in a timely manner. The incident will also be reported to the Board of Trustees.

Remote Employees

Remote employees, volunteers, contractors and Trustees must follow this policy's instructions too. Since they will be accessing our SNAPS' systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

Disciplinary Action

We expect all SNAPS' employees, volunteers, contractors and Trustees to always follow this policy. 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, employees who are observed to disregard our security instructions will face progressive discipline, even if their behaviour hasn't resulted in a security breach.

Take security seriously.

Everyone, from SNAPS' families and partners to our employees 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.

Drafted: 05/05/2025
Approved By Board: 14/05/2025
Next Review Date: 05/2026