Cyber Safety Policy

Purpose

Holden Street Neighbourhood House (HSNH) is committed to ensuring all Information & Communication Technology Systems (ICT Systems) operate in a safe manner and the organisation (by default any person or other associated entity) is not exposed to online risks. The policy seeks to protect all HSNH Committee of Governance (CoG) members, staff and attendees who use and have information stored in the ICT Systems. The guiding principles and responsibilities set out in this policy support procedural manuals and frameworks to implement this policy.

Scope

This policy applies to:

- All hardware and software used at HSNH and all related cloud-based servers and programs (ICT Systems)
- All CoG members, employees and attendees at HSNH (see definitions below).
- Any personal and sensitive information recorded on individuals.

Guiding principles

To ensure best practice in managing its ICT Systems:

The HSNH Manager will:

a) Keep an inventory of: All equipment where sensitive data is stored (computers, laptops, mobile devices, drives, USBs, disks) and organisational accounts logins (password protected) and access to programs and cloud-based servers.

b) Ensure all personal and sensitive information stored by HSNH in ICT Systems will be identified and categorised to ensure that:

- access to ICT Systems is only provided to those who require it; and
- access to personal and sensitive information is heavily restricted and protected.

c) Ensure access to ICT Systems is controlled at HSNH and only authorised users are given access.

d) Ensure passwords to ICT Systems are sufficiently rigorous to provide protection and are changed regularly.

e) Ensure software and programs used by HSNH are always current and software updates are regularly undertaken.

f) Ensure users are trained about cyber risks and how to mitigate those risks and cyber safety.

g) Ensure private data or information is only retained for the necessary time period, as required by law, before being deleted.

To ensure best practice in responding to any issues or breaches with its ICT Systems:

The HSNH Manager will ensure procedures are in place to:

- Respond and report on any suspected risks or cyber breaches (such as cyber threats, cyber incidents, hacking, phishing or viruses).
- Report any risks or suspected breaches or breaches to the CoG.
- As appropriate alert impacted people and update all cyber users of the suspected or confirmed risk or breach.
- As appropriate, alert any relevant authorities or regulatory bodies of the suspected or confirmed risk or breach.
- Engage external parties if required to respond and rectify any breach.
- Retain a record of breaches.

Responsibilities (including specific roles and responsibilities)

The **CoG** is responsible for:

- Ensuring that policy measures are in place to support management of the internal ICT Systems and minimises cyber risks.

The **Manager** is responsible for:

- Ensuring that staff and any relevant attendees understand this policy.
- Ensuring that the appropriate procedures and processes are in place to implement this policy.
- Managing any cyber risks or breaches in line with the guiding principles section of this policy.
- Reporting on any cyber risks or breaches to COG and any other relevant authorities or impacted parties.

Information Technology Administrator (where a staff member, consultant or volunteer appointed to this role) is responsible for:

- Supporting the Manager to be aware of any changes to the organisation's cyber security requirements
- Responding to any cyber security breaches or suspected breaches and

- Reporting on the organisation's cyber security management to the COG as required.

Staff and all attendees (as appropriate) are responsible for:

- Reading and following the directions of this policy and related procedures.
- Advising the Manager of any cyber risks or suspected breaches or breaches.
- Keeping login details and passwords safe
- Keeping information about HSNH's ICT Systems confidential
- Not downloading any additional software onto HSNH equipment.

Relevant legislation, regulatory bodies or guidelines and rules

- *Cybercrime Act 2001* (Cth)
- *Privacy and Data Protection Act 2014* (Vic)
- *Privacy Act 1988* (Cth)
- *Associations Incorporation Reform Act 2012* (Vic)
- *Crimes Act 1958* (Vic)
- The Adult Community and Further Education (ACFE) student information protection regulations and requirements
- Any funding body requiring us to adhere to certain privacy or cyber or other related legislation.

Procedural Framework

This policy also relates to the organisational policies and procedures outlined below:

- Cyber Security and IT Services Users Procedure
- Operations Manual
- Occupational Health & Safety Policy
- Records Management and Disaster Recovery Policy
- Privacy and Confidentiality Policy
- Working from Home Policy

Key Definitions

Cyber users: any user of Internet and or Computer based systems

Cyber safety: protects the computer/ network from malicious digital attacks.

Cyber risks: the threats posed to users of ICT systems and their owners.

Cyber breach: where one or more ICT Systems have been successfully infiltrated and / or damaged by a “bad actor”.

Cyber security: is the protection of ICT systems from attack by malicious actors.

Cyber threat: A cyber threat is any circumstance or event with the potential to harm systems or information. Some threats of concern and key cyber security trends include:

- COVID-19 themed malicious activity including phishing emails and scams;
- ransomware;
- exploitation of security vulnerabilities;
- software supply chain compromise;
- business email compromise; and
- Cybercrime.

Cyber incident: A cyber incident is an unwanted or unexpected cyber security event, or a series of such events, that have a significant probability of compromising business operations. A cyber incident requires corrective action. Examples of cyber security incidents include (but are not limited to):

- Denial-of-service attacks (DoS)
- Unauthorised access or attempts to access a system
- Compromise of sensitive information
- Virus or malware outbreak (including ransomware)

ICT systems: All hardware and software used at Holden Street and all related cloud-based servers and programs

Governing body: The Committee of Governance, comprising the Chair, Treasurer, Secretary and individual members.

Attendees: Includes volunteers, students, participants and all visitors including instructors and contractors.

Acronyms

Holden Street Neighbourhood House (HSNH)

Committee of Governance (CoG)

Adult Community and Further Education (ACFE)