Central Highlands Association of Neighbourhood Houses

Central Highlands Association of Neighbourhood Houses

Privacy and Cyber Security Policy

Document Control

Policy Title:	Privacy and Cyber Security Policy		
Policy Number:	MAN002	**Version Number:**	V2 (DRAFT)
Date Ratified:	Aug 5 2025	**Review Date:**	August 2028

Relevant standards, legislation and other documents:

- Privacy and Data Protection Act 2014 (Vic)
- Privacy Act 1988 (Cth)
- Office of the Australian Information Commissioner (OAIC)
- Office of the Victorian Information Commissioner (OVIC)
- Australian Signals Directorate

Definitions: (define key terms)	
CHANH	Central Highlands Association of Neighbourhood Houses
DFFH	Department of Families, Fairness and Housing
Members	Neighbourhood Houses (represented by managers and committees of management) funded by DFFH within the Central Highlands area
Board	Board of Governance, elected individuals responsible for the governance of the organisation
Staff	Any person employed by CHANH or volunteering at CHANH
Executive Team	CHANH President, Treasurer and Secretary

Policy Declaration

CHANH is committed to protecting the privacy and security of personal information collected, held, and managed by our organisation. We also recognise the importance of safeguarding our digital systems and data against cyber threats.

Purpose

The purpose of this policy is to ensure that information collected and held about individuals is managed in accordance with Victorian and Commonwealth privacy requirements, and that our digital systems are protected through appropriate cybersecurity practices.

The Australian Privacy Principles directs:

1. Open and transparent management of personal information
2. Anonymity and pseudonymity
3. Collection of solicited personal information
4. Dealing with unsolicited personal information
5. Notification of the collection of personal information
6. Use or disclose personal information
7. Direct marketing
8. Cross-border disclosure of personal information
9. Adoption, use or disclosure of government related identifiers
10. Quality if personal information
11. Security of personal information
12. Access to personal information
13. Correction of personal information

Australian Institute of Company Directors (AICD) and Cybersecurity Cooperative Research Centre provides the following Cybersecurity Governance Principles:

1. Set clear roles and responsibilities
2. Develop, implement and evolve a comprehensive cyber strategy
3. Embed cyber security in existing risk management practices
4. Promote a culture of cyber resilience
5. Plan for a significant cyber security incident

Further, AICD identifies the four point framework for cyber governance and resilience:

1. You cannot protect what you don't know you have (the single biggest threat is via third party websites and legacy systems - so mapping these is key).
2. Not all digital assets are equal, but they are all defendable.
3. The worst time to develop a crisis management plan is mid-crisis.
4. What is safe today may not be safe tomorrow (constant monitoring and reviewing, not a set and forget process).

These practices guide the ongoing development of CHANH cybersecurity.

Owner

This policy is the responsibility of the Board

Application

This policy applies to all employees, volunteers, contractors, and members of CHANH.

Policy Rationale

Personal information is information that directly or indirectly identifies a person. CHANH is committed to protecting the privacy of such information, including that of:

- Job applicants, employees, members, volunteers, and students (for relationship management and legal compliance)
- Individuals providing feedback, compliments, or complaints
- Contact details of partner organisations and service providers
- Required for compliance with the Australian Charities and Not-for-profits Commission (ACNC) regarding Responsible Persons

Procedures

Personal Information Handling:

OAIC Information related to Australian Privacy Principles is displayed in CHANH workspaces.

CHANH collects and manages personal information in accordance with applicable privacy laws. This includes information about:

- Job applicants, employees, volunteers, and students
- Individuals providing feedback, compliments, or complaints
- Contacts from partner organisations and service providers

All personal information is:

- Collected with consent
- Used only for the purpose for which it was collected
- Stored securely and accessed only by authorised personnel
- Disposed of securely when no longer required

Member Organisation Privacy:

CHANH recognises that members of the organisation may share personal and organisational information in the course of their involvement. CHANH is committed to protecting this information, which may include:

- Contact details
- Membership status and participation history
- Contributions to meetings, working groups, or governance activities
- Incident or sensitive information
- Feedback or evaluation perspective for CHANH
- Organisational affiliations or roles

CHANH will:

- Use member information for the purpose of managing membership, determine goals and objectives, continuous improvement, communications, and governance
- Not share member information with third parties without consent, unless required by law
- Ensure that member records are stored securely and accessible only to authorised staff or Board members
- Provide members with access to their own information upon request, and allow corrections where necessary

Members are encouraged to raise any concerns about the handling of their information with the Board.

Permitted Disclosures

CHANH may disclose personal information to:

- Service providers related to employment and entitlements
- Insurance providers for claims
- Governance and compliance reporting
- Law enforcement or emergency services where required

- Health organisations or family in emergencies
- Any party authorised by the individual

All identifying information is removed before use in statistical reporting.

Cybersecurity Practices

Current identified CHANH security risks:

- Social engineering or phishing campaigns for data, such as passwords or personal details
- Social engineering or phishing campaigns for financial scams
- Loss of access to website, repurposing of website for unintended purposes
- Insufficient password security management, principally for Microsoft, XERO and Banking Platforms, but also for other digital assets, including but not limited to CANVA, Survey Monkey and other cloud-based CHANH digital assets.

CHANH is committed to protecting its digital infrastructure through:

- Use of secure platforms (e.g. Microsoft 365, WordPress, Canva, XERO)
- Multi-factor authentication (MFA) and role-based access controls
- Regular software updates and patching
- Antivirus and endpoint protection
- Secure backup and recovery procedures
- Staff training on cyber hygiene and phishing awareness
- Annual review of cyber risks in the Risk Management Plan, continuous improvement to evolve cyber security practices

Australian Signals Directorate provides up to date advice on cybersecurity controls and reporting. ASD Information for Cyber Security is displayed in CHANH workspaces.

In the event of a cybersecurity incident:

1. Act fast, remain calm:
    a. Change passwords immediately (use strong, unique passwords)
    b. If MFA is available and not enabled, enable immediately
    c. If locked out of accounts, contact providers ASAP for recovery options.
    d. Disconnect affected devices from the internet
    e. Check antivirus software for threats
    f. Report incident to Australian Securities Directorate ReportCyber or Australian Cybersecurity Hotline on 1300CYBER1.

    g. For personal data breach support contact IDCARE for confidential suoport and tailored advice.
2. Assess the damage:
    a. What systems or accounts were accessed?
    b. As personal data been exposed?
    c. Check bank statements, email logs and cloud storage for suspicious activity
    d. If personal details have been compromised, notify people affected and contact Scamwatch to help prevent follow-up scams.
3. Strengthen defences:
    a. Update all systems and software
    b. Review who has access to sensitive data
    c. Consider cybersecurity tools like endpoint protection or dark web monitoring.
    d. Invest in training for organisation to support future incident prevention.

Artificial Intelligence (AI) Use

CHANH provides general permission for use of AI tools **only via Microsoft Copilot**. The following principles apply:

- No personal, sensitive, or confidential data may be input into AI tools
- AI-generated content must be reviewed and approved by a human
- AI is used to support productivity, not to make decisions involving personal data

Where staff identify an alternative AI provider for organisational use, permission must be sought from the Board. Permission request will include:

- Name and address of platform
- Purpose of platform
- How CHANH will use the platform
- Whether any personal details, IP or other critical information will be used in the use of the platform
- Any other identified risks

Responsibilities

Board

- Implement and monitor this policy
- Ensure compliance with privacy and cybersecurity obligations

Members

- Be informed of this policy

- Participate in reviews as required

Staff

- Implement this policy as part of their role
- Participate in training and policy reviews

Breach of Policy

A breach of this policy may result in disciplinary action, up to and including termination of employment or membership.

Related Policies and Procedures

- Employee Accommodation and Safe Workplace Policy
- Recruitment, Selection and Screening of Staff Policy
- Feedback, Compliments and Complaints Policy
- Data Breach Response Plan (to be developed if not already in place)

Addendum: Data Breach Response Plan

Purpose

This Data Breach Response Plan outlines the steps CHANH will take in the event of a suspected or confirmed data breach involving personal information. It ensures compliance with the Notifiable Data Breaches (NDB) scheme under the Privacy Act 1988 (Cth).

Definition of a Data Breach

A data breach occurs when personal information is:

- Lost
- Accessed or disclosed without authorisation
- Subject to unauthorised modification or misuse

An **eligible data breach** is one that is likely to result in serious harm to any individual affected.

Response Team

The following roles are responsible for managing a data breach:

- **Organisation Manager** – Coordinates the response and communication, assesses legal obligations and reporting
- **IT Support (internal or external)** – Assesses technical aspects and containment

Response Steps

1. Contain

- Immediately isolate or shut down affected systems
- Prevent further access or disclosure
- Secure physical records if involved

2. Assess

- Determine the type and extent of the breach
- Identify affected individuals and the sensitivity of the data
- Assess the risk of serious harm

3. Notify (if required)

If the breach is likely to cause serious harm:

- Notify the Office of the Australian Information Commissioner (OAIC) using the NDB form
- Notify affected individuals with:
    - A description of the breach
    - The type of information involved
    - Recommended steps for protection
    - Contact details for further information

4. Review

- Investigate the cause and effectiveness of the response
- Update security measures and policies
- Document the incident and lessons learned

Record Keeping

All data breaches, whether notifiable or not, must be documented in CHANH's internal incident register, including:

- Date and time of breach
- Description of the breach
- Actions taken
- Outcome and follow-up

Training and Awareness

Staff will receive training on:

- Recognising and reporting data breaches
- Following this response plan
- Preventative cybersecurity practices