POLICY – CYBERSECURITY

Policy number	N/A	Version	1
Drafted by	Karen Zirkler	Approved by Board on	30 September 2025
Responsible person	Karen Zirkler	Scheduled review date	June 2027

1. Overview

Cybersecurity is the practice of protecting information systems, networks and data from unauthorised access, use, disclosure, disruption, modification or destruction. Cybersecurity is essential for protecting Southern New England Landcare and member data. Without proper measures and without every member of staff securing their devices, services and networks and being cyber-vigilant, data can be compromised, and the organisation and its reputation could be seriously or irreparably damaged.

Southern New England Landcare's partners and members trust us to keep their data safe. This policy ensures employees, directors, volunteers and contractors understand their responsibilities and our members, partners and stakeholders' expectations of them to keep this promise.

2. Purpose

The purpose of this policy is to stipulate what is expected of staff, directors, tenants, volunteers and contractors in helping secure the organisation's data, devices and network. Compliance with this policy helps ensure that the organisation is doing everything possible to keep all sensitive and personal data protected and to maintain our reputation as a secure operator.

3. Scope

This policy applies to all persons (employees, tenants, directors, volunteers, temporary workers, contractors and agents acting on behalf of Southern New England Landcare) that use or have access to the organisation's devices, network, or any of Southern New England Landcare's data in digital form.

4. Policy

4.1 Protection of data

4.1.1 Confidential information

All employees, tenants, directors, volunteers and contractors must take all reasonable precautions to protect the confidential information they gather, store, manage or otherwise encounter during their work for Southern New England Landcare Ltd.

Employees, tenants, directors, volunteers and contractors shall not share any confidential information with any party outside the organisation, or any person within the organisation who is

not authorised to have access to the information, without the explicit permission of their line manager.

Confidential information includes, but is not limited to:

- Lists of members (existing and prospective)
- Unpublished financial information
- Any other unpublished organisational or partner data.

4.1.2 Personally identifiable information

All employees, tenants, directors, volunteers and contractors must take all reasonable precautions to ensure that personally identifiable information is collected, stored, used and shared in accordance with all applicable state and federal data-protection regulations and requirements, as well as the organisation's rules.

Personally identifiable information of employees, partners, members or any other person must not be shared with any third parties without the consent of the person whom the data relates to, and without a compelling reason to do so.

Personally identifiable information includes, but is not limited to:

- Full names of individuals
- Phone or mobile numbers of individuals
- Email addresses of individuals
- Postal addresses of individuals
- Payment (e.g. credit or debit card) details of individuals.

4.2 Protection of devices

All employees, tenants, directors, volunteers and contractors must take all reasonable steps to protect the physical and digital security of Southern New England Landcare's electronic devices, and of any electronic device used to access the organisation's data or network.

All employees, tenants, directors, volunteers and contractors must:

- Ensure that all devices under their control are protected with a secure password or other form of authentication, such as fingerprint or facial recognition
- Set all devices under their control to automatically lock themselves after no more than five minutes without activity
- Never leave devices under their control unattended in public places
- Report any security issue relating to a device in their control to the organisation without undue delay
- Install all operating system, antivirus and antimalware updates and patches as soon as reasonably possible
- Take all reasonable steps to never allow any person not associated with the organisation to use or access a device under their control where such access could facilitate a breach of the organisation's cybersecurity policy
- Never download any illegal or potentially malicious software using the organisation's network or an organisation-owned device
- Hand back any electronic devices belonging to the organisation once they are no longer needed.

4.3 Protection of networks

All employees, tenants, directors, volunteers and contractors must take all reasonable steps to maintain the integrity of the organisation's networks and ensure that no unauthorised party is able to gain access to the networks.

All employees, tenants, directors, volunteers and contractors must:

- Only access the organisation network from a device owned by the organisation or one that they have been given explicit permission by the CEO to access the organisation's network from
- Ensure that all devices that access the organisation's network are running the latest version of the operating system and latest antivirus software updates
- Utilise a Virtual Private Network or any other software that has been provided to them by the organisation to help ensure the integrity of the organisation's networks.

4.4 Email security

Email must be used responsibly to ensure that the organisation's networks, services or data are not compromised due to insecure use. All employees, tenants, directors, volunteers and contractors must take all reasonable steps to ensure that their use of email minimises the risk of (i) downloading malicious software, (ii) giving up personal or confidential information, or (iii) enabling unauthorised access to the organisation's systems.

All employees, directors, volunteers and contractors must:

- In cases where they have been provided with one, only send and receive organisation-related information and correspondence from their official organisation-provided email address
- In cases where they have been provided with one, protect their organisation email address with a secure password and multi-factor authentication if available
- Never send or forward any confidential or personal information to any third-party email address without the explicit permission of their line manager
- Exercise caution and take reasonable precautions when clicking on links and attachments in emails to reduce the risk of downloading malware or providing unauthorised system access
- Never open an attachment in an email from an unknown source
- Never use email to send passwords or other cybersecurity credentials.

4.5 Internet security

The internet must be used in a responsible manner and only as and when required for organisational purposes. Employees, tenants, directors, volunteers and contractors are responsible for ensuring that their use of the internet does not expose Southern New England Landcare's electronic devices, networks, or data to unauthorised access or damage from malicious software.

All employees and tenants must:

- Use an up-to-date, secure web browser when accessing the internet
- Ensure their electronic devices are running up-to-date antivirus software and have the latest operating system updates and patches installed
- Limit personal use of the internet on Southern New England Landcare's devices and the company network to a reasonable minimum

- Never use the organisation's network or devices to access illegal or potentially malicious websites or content
- Never use the organisation's network or devices to access pornographic, offensive or violent content
- Report any potential security incident to their line manager and/or IT support team without any undue delay.

5. Compliance

5.1 Compliance measurement

The CEO/line manager/IT support team will verify compliance with this policy through any methods deemed appropriate including, but not limited to, business tool reports, internal and external audits and feedback to the policy owner.

5.2 Exceptions

Any exceptions to this policy must be approved by the CEO in advance in writing.

5.3 Non-compliance

Any employee, tenant or contractor failing to comply with this policy may be subject to disciplinary action, up to and including termination of their employment contract or service agreement.

Any director or volunteer failing to comply with this policy may be subject to disciplinary action, up to and including termination of their membership and services.

6. Authorisation

Em Prof Nick Reid
Chair, Southern New England Landcare Ltd
30 September 2025