Use and Protection of Technology Resources Policy

Preamble

Computer and information systems underpin all Spiritualism New Zealand's (SNZ'S) activities, and are essential to its membership services, marketing, communication and administrative functions. This policy provides a framework for the management of information security throughout SNZ, including establishing specific requirements for the appropriate use of SNZ's technology resources.

This policy should be interpreted broadly and to include the use of new and developing technologies not explicitly listed in this policy.

In general, acceptable use means respecting the rights of other users, the security and integrity of the physical and virtual resources and all relevant license and contractual agreements of all information technology (IT) resources.

This policy applies to all IT users and resources, including but not limited to:

- All those with access to the SNZ's information systems or any underlying SNZ-provided network connectivity either wired or wireless, including staff, contractors and volunteers but not the general public.
- All external parties that provide services to SNZ in respect of information processing facilities and providing services, including users associated with those third parties who access SNZ's systems.
- Any devices attached or connected any SNZ IT networks and systems (including servers, PCs, portable computers, laptops, notebooks, tablets and mobile / smart devices, printers, scanners, external drives and other portable media).
- All technology systems supplied by SNZ or used by or licensed to SNZ to deliver its services.
- Any system that hosts SNZ information including cloud environments and software-as-a-service applications, including social media systems.
- Data and information assets accessed through any of the above (regardless of where they are located or how they are processed or communicated).

Aims of this Policy

This policy seeks to:

- Protect the confidentiality, integrity, and availability of information to support SNZ in functioning effectively and efficiently and ensure users have access to the information they require to carry out their work.

- Protect against unauthorized system access that may result in harm to SNZ or its stakeholders.
- Ensure there is no unauthorised disclosure of information, use, modification or other outcome which could potentially damage SNZ's reputation and/or cause financial loss.
- Ensure users understand the importance of information security and how to exercise appropriate care when handling SNZ information or using SNZ provided networking connectivity through appropriate training.
- Ensure appropriate resources and processes are in place to identify and manage information security incidents, including recording and reporting on any breaches of information security.
- Ensure information security risk assessments are performed on a regular basis to identify key information risks and ensure these risks are managed within tolerance.
- Apply industry best practice as far as practical for all matters relating to information security.
- Establish responsibilities and accountability for Information Security.
- Avoid breaches of any statutory, regulation or contractual obligations, including the Crimes Act 1961, Harmful Digital Communications Act 2015, Privacy Act 2020, The Unsolicited Electronic Messages Act 2007.
- Protect the integrity of information by preventing accidental or unauthorised alteration of information.
- Ensure the availability of information by protecting against accidental or malicious destruction or deletion.

To these ends it also seeks to:

- Define what constitutes acceptable use of SNZ's technical resources and the obligations on those using the resources.
- Provide guidance on what constitutes unacceptable use of SNZ's IT resources.
- Ensure the confidentiality, integrity, availability, reliability, security, and performance of information technology systems.
- Ensure the use of information technology systems is consistent with the principles and values that govern the use of other SNZ services.

Policy

Spiritualism New Zealand provides staff, volunteers, contractors and other users with technological systems and resources in order to perform their roles effectively and maximize their productivity. However they need to use these resources responsibly so their use does not negatively impact others sharing this technology, nor bring SNZ into disrepute if viewed by an independent person.

1. Information security

1.1. All users have individual and shared responsibilities for protecting SNZ information, from unauthorised access and use.

1.2. All users are responsible for protecting their SNZ passwords (passwords to SNZ systems and /or networks) and other access credentials from unauthorised use. Credentials must not be shared without explicit, written permission of the SNZ Board (the Board) or their delegate and only in exceptional circumstances.

1.3. All access to and use of SNZ information and systems must be for authorised SNZ purposes only. They are not to be for private commercial purposes or activities. Personal use should be limited to essential communications only.

1.4. All access to and use of SNZ provided network connectivity or system by any 3rd party must be authorised by the Board in advance. Failure to comply with this and other relevant policies will result in the disconnection and removal of access to SNZ provided system.

1.5. SNZ confidential information must be protected by the use of passwords or pin codes or encryption as appropriate, on any user's computer or portable device irrespective of whether the device is owned by SNZ or the user.

1.6. Passwords should be a minimum of 8 characters long composed of letters and at least one number and one special character. This is to ensure a password cannot be easily recognised or copied by anyone else.

1.7. All systems and especially Internet facing systems must implement multi-factor authentication (MFA) for Administrator access and user access, where this is available.

1.8. Passwords and SNZ’s data should not be exposed to public view. SNZ’s technology resources should not be left such that they can be accessed or viewed by anyone who does not have SNZ’s consent / authorisation to so access. This may involve leaving the device “locked” if leaving it unattended for any period of time or logged off the application.

1.9. Access to Information and systems is controlled and a principle of need to know and least privilege will be applied.

1.10. Critical information assets are categorized according to sensitivity and protected accordingly.

1.11. Technology risks associated with information systems are regularly identified, assessed, managed and mitigated.

1.12. All new systems and those existing systems undergoing a significant upgrade/change must undergo a security assessment and gain approval from the Board before being implemented. Where appropriate a privacy assessment must also be completed for all new systems and those undergoing significant upgrade/change.

1.13. All servers and services storing SNZ confidential information must be protected against improper access.

1.14. Systems and applications must be kept up to date on all devices that process or store SNZ information or are connected to any SNZ provided network.

1.15. Systems and applications are developed, procured, managed and disposed of securely during their lifecycle.

1.16. Unsuccessful attempts to log on to any application or server that processes or stores SNZ information will be limited.

1.17. Applications and systems that contain SNZ information must be properly disposed of so that the information cannot be retrieved or reassembled when no longer required.

1.18. SNZ will conduct appropriate due diligence to ensure that third parties who store or have access to SNZ information are capable of properly protecting the information. Records of all such systems and access will be kept.

1.19. Any actual or suspected loss, theft, or improper use of, or access to, SNZ information must be reported to the Board soon as practicable.

1.20. SNZ will comply with all legal requirements and other agreements where applicable following a compromise of any system.

1.21. All users of SNZ systems and any network connectivity, must comply with reasonable requests for access to systems and logs to assist in the investigation and resolution of cyber and operational incidents by SNZ and its contractors.

2. Acceptable use

2.1. Acceptable use of SNZ IT resources includes:

a) Accessing and using IT systems and facilities for legitimate SNZ work purposes.

b) Accessing information from the Internet and using general Internet services for legitimate work purposes.

c) Undertaking activities that are otherwise deemed unacceptable if they have been explicitly authorised by the SNZ Board.

d) Using personal devices for legitimate SNZ work purposes when at home or travelling.

2.2. Unacceptable Use of SNZ’s IT resources includes, but is not limited to:

a) Not keeping your passwords and access codes confidential.

b) Sending messages or distributing content which brings SNZ into disrepute or compromises its credibility, integrity or standing.

c) Interfering with SNZ in meeting its legal obligations.

d) Creating, viewing, saving or distributing material that could be considered offensive, obscene, indecent, illegal or reflect badly on SNZ.
e) Deliberately creating, introducing or distributing computer viruses or other malicious software.
f) Excessive use of SNZ IT resources or otherwise deliberately downgrading their performance.
g) Monitoring, probing for security vulnerabilities, intercepting, altering, hacking or attempting any unauthorised access to SNZ systems, networks, and data unless explicitly authorised by the Board.
h) Improperly and inappropriately revealing, disclosing or sharing confidential personal or proprietary information through websites, blogs, discussion forums, email, social media etc.
i) Pirating, plagiarizing, using, copying or distributing information in contravention of copyright or other laws.
j) Using SNZ's technology resources for violence, criminal activity or dishonest purpose.
k) Annoying, harassing or defaming others, distributing spam, spreading malicious rumours and other antisocial behaviour.
l) Sharing or disclosing personal user identities, passwords, security tokens etc. with anyone else.
m) Impersonating or making other inaccurate or false representations as to an identity or the identity of others.
n) Storing confidential or sensitive SNZ information on a personal device or non-SNZ storage location unencrypted without prior Board approval.
o) Using SNZ IT resources to work on behalf of other organisations, including charities and not-for-profit organisations, without prior approval from the Board.
p) Changing IT-related resources without prior approval of the Board. This includes the installation and use of unauthorised services or software to perform SNZ work.

3. Resigning from a technology-user role

3.1. Upon resigning or otherwise terminating form a Board position, volunteer or contractor role that used SNZ technology resources, the technology user must:

a) Delete any SNZ files and emails not required by SNZ for its "business" purposes. They must transfer their remaining SNZ files, data and applications back to SNZ and the person replacing them in their role (or other designated person). This may include emails.

b) Return any technology equipment owned by SNZ back to SNZ is returned to SNZ and their replacement (or other designated person).

4. Other user obligations under this policy

4.1. To ensure the IT resources continue to be effective for SNZ work purposes, all users are required to take adequate care of the resources they use. Any faults, damage or incidents where service is compromised are to be reported to Board officers at the earliest opportunity.

4.2. Users must be respectful of the personal rights of others while using information technology resources.

4.3. Users must commit themselves to comply with all of the licensing, contractual and copyright obligations and laws of New Zealand.

4.4. All users, regardless of their physical location or the devices they use, must maintain and follow safe security practices so as not to jeopardize SNZ’s information technology resources in any way.

4.5. Users should also be vigilant of cyber security threats and should take reasonable steps to protect themselves.

5. Right to Monitor

5.1. Users are granted use of electronic information systems and resources to conduct SNZ services, administration and other authorised activities. SNZ reserves and retains the right to access, inspect, monitor and audit all information technology resources covered by this policy.

6. Consequences of breaching the Use and Protection of Technology Resources Policy

6.1. Users who misuse any information technology resources and services may have their access suspended without notice.

6.2. Aiding or coercing breaches of this policy will be deemed as having equal responsibility for the action of the perpetrator.

7. Responsibilities

7.1. Shared responsibility for Information Security rests with all staff, contractors and volunteers.

7.2. Users of SNZ’s technology systems, resources and confidential information have responsibility for:

a) Keeping their username and password secure.

b) Ensuring all SNZ information is stored on secure systems.

c) Reporting any potential and suspected breaches of security to the Board.

d) Informing the Board in the event of lost technology assets, damage or security incidents.

e) Returning all SNZ files, emails, and system access to SNZ upon leaving.

f) Complying with the Use and Protection of Technology Resources Policy.

7.3. The Board is responsible for:

a) Ensuring best practice Information security is followed.

b) Ensuring all staff, volunteers and contractors are informed of and adhere to the Use and Protection of Technology Resources Policy.

c) Security policies and procedures

d) Security awareness and training

e) Cyber incident / data breach management

f) Third-party vendor management

g) Ensuring all access rights are removed from any user who is leaving the organisation or technology-user role.

h) Data Governance oversight

7.4. The Board has overall responsibility for:

a) Acquiring technology resources to meet its service and administration needs, and maintaining them and their licenses.

b) Ensuring all software and technology services used are licensed to SNZ and that proof of all such licences are held.

c) Ensuring information technology continues to meet SNZ's requirements.

7.5. Where Board members have primary liaison responsibilities for certain technology services or software, they have the responsibility to ensure it remains fit-for-purpose and is supported in an efficient manner, or it is escalated to the Board.

Acceptance of Spiritualism New Zealand's Use and Protection of Technology Resources Policy

8.

I have had the opportunity to review and discuss this "Use and Protection of Technology Resources Policy". I have read, understood and accept the above Policy document relating to the use and protection of Spiritualism New Zealand's technology property.

Full Name: ____________________________

Designation: ____________________________

Signature: ____________________________

Date: ____________________________