Policy Name

Privacy Policy

1 Purpose

The purpose of this policy is to communicate The Theosophical Society in New Zealand's need to use, manage and store personal information about our employees and members in a manner consistent with employees' and members' privacy rights. This policy is intended to be consistent with the obligations set out in the Privacy Act 2003.

2 Organisational Scope

This policy applies to:

- All employees and former employees of TSNZ.;
- Any members of TSNZ;
- Any person engaged or contracted under a contract for services to do work with TSNZ;
- Any volunteer delivering works or services for TSNZ.

For the purposes of this document the terms 'employee' and 'employees' include all of the above.

3 Definitions

For purposes of this policy, unless otherwise stated, the following definitions shall apply:

Employee[s]:	Employee[s] include staff, volunteers and contractors who work for the National Office of TSNZ.
Privacy Officer:	National President
TSNZ:	The Theosophical Society in New Zealand Inc.

4 Policy Principles

TSNZ is an organisation that is required to abide by the Privacy Act.

TSNZ has obligations to manage information about employees and members appropriately.

5 Information Records

5.1 Membership Information

5.1.1 Who TSNZ Collect information from

Members, when they provide their personal information to us in joining TSNZ, including via the website and any related service, through any registration or subscription process, through any contact with us (e.g. telephone call or email), or when they buy or use our services and attend TSNZ events

5.1.2 Personal Information Collected

- Full name.
- Contact details (including address, telephone and email address).
- Date of birth if under 18.
- Date of joining/re-joining.
- Gender.
- Diploma Number.
- Branch membership of.
- Subscription to New Members letters.
- Membership status.
- Event Registrations.

5.1.3 Purpose of Collection

The purposes for which personal membership information is collected and used by TSNZ include:

(a) To comply with the Incorporated Societies Act (1908)

(i) Must keep a register of its members.

(ii) The register must contain the names and addresses of the members, and the dates when they became members.

(iii) TSNZ must, on request by the Registrar, send to the Registrar a list of the names and addresses of its members, accompanied by a certificate by an officer of the society certifying that the list is correct.

(b) To comply with the rules of the International Headquarters of the Theosophical Society at Adyar, Chennai, India, who require members applications be sent to them for their records.

5.1.4 How we use personal information

(a) To verify a members identity.
(b) To verify a members membership status.
(c) To be able to inform members of events at TSNZ.
(d) Enable the sending of TheoSophia, our quarterly magazine and newsletters, including contacting them electronically (e.g. by text or email for this purpose)
(e) To allow members to be sent voting slips and information for elections of TSNZ Officers and Governance Board or referendums.
(f) To be able to inform National Society members when subscriptions are due and to collect subscriptions, including authorising and processing credit card transactions
(g) To respond to communications from members.
(h) To conduct research and statistical analysis (on an anonymised basis)
(i) To protect and/or enforce members legal rights and interests, including defending any claim for any other purpose authorised by you or the Act.

5.1.5 Disclosing personal information:

We may disclose your personal information to:

(a) A Theosophical Society Branch or Lodge within New Zealand for upkeeping of their membership records.
(b) To the International Society at Adyar, Chennai, India for their records.

(c) Police, or other party in the nature of pre-employment checks .
(d) Any person authorised by the Act or another law (e.g. a law enforcement agency)
(e) A business that supports our services and products may be located outside New Zealand. This may mean your personal information is held and processed outside New Zealand, for example, cloud storage or book sales.

5.1.6 Security of Information

(a) TSNZ will take reasonable steps to protect the personal information it collects from misuse and loss and from unauthorised access, modification or disclosure. Personal information is normally stored at TSNZ in electronic form, which is protected from unauthorised access by a password system. TSNZ staff have access to personal information only to the extent that it is required for them to carry out their duties.
(b) Personal information in hard-copy form is also be stored in a secure place.

5.1.7 A Member Requesting Access to Information his/her Personal Information

(a) TSNZ verifies the identity of the requestor to ensure it is the individual concerned or his/her agent.
(b) TSNZ responds to such requests as soon as practicable.

5.1.8 Misuse of Personal Information

Without limiting the definition of misuse of personal information, the following practices are unacceptable to TSNZ:

(a) Intentionally breaching the *Privacy Act,* the *Official Information Act* or the access restrictions imposed by the *Public Records Act*;

(b) Reading or copying personal information to which the reader/copier has no authorised access;

(c) Divulging personal information given under an express undertaking it will remain confidential or, intentionally divulging personal information to any person who is not an authorised recipient of that information without lawful excuse;

(d) Deliberately introducing false or misleading material into TSNZ database or file/record, or falsifying such records or deleting such records without authorisation.

(e) Using personal information for any purpose other than the purposes identified unless the individual has given explicit, informed consent to do so.

5.2 Employee Information

5.2.1 Personal Information Collected

(a) TSNZ collects and retains different types of personal information in respect of those individuals who seek to be, are, or were employed or engaged by TSNZ, including the personal information contained in:

1) Resumes/CVs;
2) Applications for employment and supporting documentation;
3) References;
4) Interview notes;
5) Offers of employment;
6) TSNZ policy acknowledgment forms;

7) Payroll information, including but not limited to IRD numbers and tax codes, bank account details for wage / pay deposit etc.;
8) Pre-employment checks, including but not limited to health checks and police vetting forms;
9) Health and safety forms relating to benefits, long and short term disabilities, medical care and emergency contact information;
10) ACC information;
11) Performance assessments and agreements;
12) Disciplinary information (including health checks).

(b) In addition to the examples above, personal information also includes information such as full names, residential addresses, telephone and mobile number(s), personal email addresses, dates of birth, as well as any other information necessary to enable TSNZ to meet its obligations as an employer.

(c) Personal information will be sought wherever possible directly from the individual concerned, unless the employee agrees otherwise.

5.2.2 Use and disclosure of personal information collected

(a) TSNZ may share employees' information with other TSNZ employees, consultants, and other parties who require such information to assist TSNZ with establishing, managing or terminating TSNZ employment relationship with its employees, or for purposes associated with the Protected Disclosures Act 2000.

(b) TSNZ must comply with Privacy Principle 11 of the Privacy Act 1993 which provides that information should not be disclosed to third parties unless:

- The disclosure is directly related to the reason the information was collected in the first place;
- The employee has authorised the disclosure;
- The information is publicly available;
- Disclosure is necessary for the maintenance of the law or for legal proceedings (e.g. for the Employment Relations Authority);

  or
- Where possible criminal or other unlawful activity is suspected.

5.2.3 Protection of Personal Information

(a) TSNZ endeavours to maintain physical, technical and procedural safeguards that are appropriate to the sensitivity of the employees' personal information. These safeguards are designed to prevent personal information from loss and unauthorised access, copying, use, modification or disclosure. These include:
  - Keeping employees' personnel files in hardcopy which is stored under lock and key, and restricting access.
  - Limiting access to employees' personal information on its electronic systems by restricting access.

(b) It is important that the information held in TSNZ records is both accurate and current. If an employee's personal information changes during the course of their employment the details of the changes need to be recorded.

(c) If an employee believes that the information held by TSNZ about him or her is incorrect, the employee in the first instance should correct the information. If the information is not corrected, the employee may make a written request to TSNZ's to correct the information.

(d) If TSNZ does not agree that the information is incorrect, the employee may have attached to that information a written statement from the employee as to what they believe the correct information to be.

5.2.4 Access to personal information

(a) All employees may request to see their employee file held by TSNZ. They should contact their privacy officer to arrange a suitable time to do so.
(b) TSNZ employees can request access to their personal information verbally or in writing. Employees do not have to explain why they want to view their information, though it is often helpful to do so. If the request is urgent, the employee must specify why it is urgent.
(c) TSNZ will provide access to the information in the way preferred by the employee unless this would impair efficient administration, breach a legal duty, or breach an interest protected by one of the withholding grounds under the Act, which TSNZ would then give reasons for the decision. TSNZ will provide access without undue delay and will give reasons for a decision to withhold information.
(d) Employees will be able to view and copy their personal information with the policy officer present.
(e) Employees are entitled to all other personal information held by the TSNZ about them, including (but not limited to) their wage and time records, holiday and leave records and information (whether in written, electronic or other form).
(f) TSNZ may withhold information pursuant to Part 4 of the Privacy Act 1993. The reasons for which information may be withheld include, but are not limited to, the following:

- Giving access to information would involve the unwarranted disclosure of personal information about another person or employee;
- The information is protected by legal professional privilege; or
- Giving access to the information could hinder an investigation into a criminal offence.
- If information has been subject to a complaint enquiry or panel discretion may be used in these cases to either release of not release this information.

5.2.5 Electronic Information Systems

(a) TSNZ employees are provided with access to computerised information and tools, usually via a personal computer, so they can carry out the duties required.
(b) Employees are assigned a system ID (Username and Password). That employee is accountable for use of their system ID and therefore should not disclose their system password to any other person in TSNZ except in exceptional circumstances and never to an external party.

5.2.6 Email and Internet

(a) TSNZ sets out the conditions under which employees may use e- mail and internet services. It is acknowledged that personal use of the internet may occur where that does not disrupt the delivery of TSNZ services.
(b) These services have been installed to help employees carry out their work and employees are encouraged to make full use of them for this purpose. However, they can be used in ways that put at risk the availability of computer services, the integrity of TSNZ information and the credibility of TSNZ as a not-for-profit organisation. The Management reserves the right to:
    - Monitor, intercept, inspect and if necessary disclose e-mails transmitted by, received by, or stored using TSNZ computers or equipment;
    - Monitor and if necessary disclose the history of Internet and World Wide Web pages and sites accessed using TSNZ computers or equipment.

(c) Monitoring activity will be to the extent necessary to protect TSNZ's interests and those of its employees in light of its legal obligations, to maintain business continuity, and to ensure the effectiveness of the policies on electronic media and systems.
(d) Monitoring and inspection of past usage of e-mail and internet services will be undertaken if there is good reason to suspect unreasonable or prohibited use of e-mail or internet services, and/or if responding to a legitimate request to do so by a third party;

5.2.7 Applicant Information

(a) Information collected about applicants (internal or external) during a recruitment process is treated in strict confidence. This confidence extends to applications, interviews and all selection and related administration processes. Officers are to ensure the interview panel are aware of this requirement.
(b) Information regarding successful candidates is securely stored electronically and is viewable only by TSNZ Officers. Unsuccessful applicants' information is retained for a total of 12 months and then destroyed. The reason for this is that this is the timeframe for an unsuccessful applicant making a complaint pursuant to the Human Rights Act 1993.
(c) This information includes Application Forms, CV's, Interview Notes and Pre- Employment Screening, Psychometric testing, qualification checks, eligibility to work in New Zealand, health and safety assessments, health information and any Police or Ministry of Justice background checks carried out and other evaluative material.

5.2.8 Retention of Personal Information

TSNZ will retain employee's personal information after the termination of the employment relationship as required by the Public Records Act 2005, the Employment Relations Act 2000, the Holidays Act 2003 and the Tax Administration Act 1994.

5.3 Information in the Workplace

5.3.1. Information Devices

(a) All information held on devices, the network, whether in private file storage space or in shared file storage space, is potentially available to the public, unless there are reasons, as defined by statute, for withholding it.
(b) Employees must ensure that devices are protected or locked by appropriate passwords so that in the event of theft or loss, the information can not be accessed.
(c) Employees must never place information on the network or their computer that would embarrass or discredit themselves, other staff members, or TSNZ should any member of the public gain access to it. This includes e-mail messages.
(d) Information received or created in the course of performing duties belongs to the TSNZ irrespective of what device it is stored or used on, and who owns the device.

5.3.2 Taking Information Outside the Workplace

(a) When using a TSNZ laptop or other electronic device for work off site, users have access to TSNZ's standard office programmes, their own personal space on the network and access to shared space on the network as required.
(b) Users must seek advice if issues of public access to information arise, or are likely to arise.

5.3.3 Unsolicited Messages

(a) The Unsolicited Electronic Messages Act 2007 provides that when TSNZ sends commercial messages it must have the consent of the people to whom it is sending the message. It is up to TSNZ to be able to prove that it has the person's consent. Consent can be:

- express (e.g. ticking a box on a website to have a newsletter sent to them);
- deemed (e.g. TSNZ could send emails about an event at in Auckland to branches that have published their work email addresses in advertising brochures and have not stated that unsolicited messages are not to be sent to that address); and
- inferred (when a person has not directly instructed TSNZ to send them a message, but it is clear there is a reasonable expectation that messages will be sent – it may be possible to infer consent of persons on existing address lists who have not 'unsubscribed', depending on the length of time over which TSNZ has been sending emails to the person, and how it came about that TSNZ is sending the emails. The Department of Internal Affairs (DIA) suggests that if an organisation is not confident that the existing relationship between the organisation and the email recipient is strong enough to infer consent, it should obtain express consent from that person).

(b) Where TSNZ has a recipient's consent then it is not sending unsolicited commercial electronic messages (spam). However, it needs to ensure that such emails accurately identify TSNZ, as the sender of the message (this does not necessarily need to include an individual's name), and that the message includes a functional unsubscribe facility, to enable the recipient to advise TSNZ that no further messages are to be sent to the recipient. If TSNZ does not have a person's consent to send a electronic message then it needs to obtain consent first. TSNZ can communicate with that person by a means other than email or text message to seek consent, or it could send an email or text to the person to seek consent, provided the email does not contain any other links or information of a commercial nature.

5.3.4. Unintended Disclosure of Information

If an employee becomes aware of an unintended release of information or transmission of information to an unintended recipient, this must be reported to their National President so that appropriate action to recover the information, or ensure the information is deleted and not passed on further can be taken.

6 Legislative Compliance

The Society is required to manage its policy documentation within a legislative framework. The legislation directing this policy is the:

1. Privacy Act 1993
2. Protected Disclosures Act 2000
3. Unsolicited Electronic Messages Act 2007
4. Official Information Act 1982
5. Incorporated Societies Act 1908
6. Public Records Act 2005
7. Public Records Act 2005,
8. Employment Relations Act 2000,
9. Holidays Act 2003
10. Tax Administration Act 1994

7 Contact Person

TSNZ's privacy officer is the National President.

All requests pursuant to the Privacy Act 1993 and all questions regarding privacy issues must be directed to the privacy officer in the first instance.

8 Review Date

Approval Date: April 2019

Review Date: 2022