PRIVACY POLICY

THE INVESTMENT STORE LIMITED

Version	Final v3.0
Last Updated	14/03/25
Next Review	September 2025

Contents

Version Control

Author/Contributor	Version	Date	Comments
Elizabeth Ginever / Matt Mimms	Final v1.0	26/11/2020	Final for approval by the Director
Matt Mimms	V2.0	01/08/2022	Updated
Matt Mimms	V3.0	14/3/25	Updated

1. Introduction

The new Privacy Act 2020 comes into force effective 1 December. It is an extension of the previous Act and builds on the previous principles-based approach. There are now 13 Principles which are detailed in Annexure 1, Privacy Principles

2. Personal Information that is collected

TISL typically only deals with financial intermediaries and institutional investors (wholesale clients).

TISL collects personal information directly from the client concerned and/or their authorised representative. The information collected includes name, address, contact details and diary notes of relevant meetings and interaction.

TISL only collects personal information for lawful purposes connected with the TISL's functions and activities, and only where the collection of such information is necessary for those purposes.

Clients can choose not to provide their personal information to the TISL. However, this will limit the services TISL can provide to the client. If clients do not provide TISL with necessary personal information, TISL may have to refuse or cease to provide the client with products or services.

3. Method of collection of personal information

TISL will only collect personal information by lawful and fair means and not in a way that may be unreasonably intrusive. Wherever possible, TISL collects personal information directly from the client when the clients provides information to TISL. TISL may also collect personal information from third parties where the client has authorised the relevant collection such as any authorised representatives. TISL may also collect personal information from publicly available sources.

Clients will give consent to use their personal information. Prior to giving consent TISL will ensure that the request for consent is given in an intelligible and easily accessible form and includes the purpose for the data processing.

TISL will take reasonable steps to ensure that the client is aware that the:

(a) information is being collected;
(b) purpose for which the information is being collected;
(c) intended recipients of the information;
(d) name and address of the agencies that are collecting and holding the information;
(e) collection of the information is authorised or required by or under law, and if so
    (i) the particular law; and
    (ii) whether the supply of information is voluntary or mandatory;
(f) consequences of not providing the information; and
(g) rights of access to and correction of information

4. Purposes of collecting, holding, using and disclosing personal information

TISL maintains a client database which is used for mailing and record keeping (diary notes) purposes. This is limited to name, address, contact details and diary notes of relevant meetings and interaction.

This is kept for the following types of clients, and in order for TISL to maintain high levels of service, and in the case of its fund manager clients, assist in meeting it's contractual obligations :

a. Financial intermediary and institutional investors clients and others that we deal with in our marketing activities
b. Fund manager client contacts
c. Other industry participants (e.g. industry associations etc)
d. Other suppliers (such accountant, IT, legal, compliance providers)

TISL is also party to and holds some information from their fund manager clients and in respect of the fund manager's underlying clients/investors. This is typically made available to TISL for the purposes of reporting and understanding the source of client flows.

5. Disclosure of personal information

TISL will not disclose information except in accordance with the Privacy Act.

TISL discloses client information to its domestic and Australian based fund manager clients (note that each of our contracts has a confidentiality requirement) from time to time and in accordance with the relevant contract. In addition;

- TISL can only provide client (investor) information from fund managers to advisers if they are the unitholder or they are the adviser on record (this information should be attained from the fund manager)
- TISL can only provide client information to individual investors (w'sale or retail) if they are the unitholder or have authority – in most circumstances, TISL should refer any such enquiries directly to the fund manager – where this is not possible, TISL should identify the investor by asking for full name, DOB, address and ascertain their familiarity with their investment.

TISL may, from time to time, request clients' (or their personal representatives') consent for TISL to use and/or disclose personal information for specified purposes. A request for consent (e.g. via an application form) will be given in an easily understandable and accessible form and includes the purpose for the data processing.

6. Protection of personal information

TIS uses such security safeguards as reasonable in the circumstances to protect information from misuse, interference and loss, and from unauthorised access, modification or disclosure. TISL takes precautions including:

(a) restricting access to personal information stored on TISL's servers;
(b) imposing confidentiality requirements on its employees;
(c) imposing confidentiality requirements on its fund manager clients (where a marketing contract and agreement is in place);
(d) requiring that its contractors and agents take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure;
(e) implementing electronic security systems, such as firewalls;
(f) ensuring that servers containing client information have security measures such as password protection; and
(g) controlling access to TISL's office
(h) taking reasonable steps to protect "unique identifiers" from being misused. (Unique identifiers are individual's numbers, names or other forms of identification allocated to people by organisations, such as IRD numbers, bank client numbers, driver's licence and passport numbers.)

TISL stores data mainly on the Cloud (this service is provided by Lucidity NZ and uses MS 365).

Some data is stored on desktop devices as a back-up.

TISL uses Gotowebinar (webinars). This software, used for webinars etc typically requires users to input their name, company and e-mail address as part of the registration process and any questions in relation to a specific webinar. Gotowebinar is a UD based software provider. Gotowebinar's privacy policy is available here - https://www.goto.com/company/legal/privacy/us
TISL uses Campaign Monitor (e-mail software). TISL will import basic contact information to create subscriber lists (name, company, e-mail address only). Subscriber lists are regularly updated and old ones deleted. The e-mail software that TISL uses (Campaign Monitor) allows TISL to view recipient's engagement with any campaigns/emails sent. This extends to whether a recipient opens the campaign and which if any links are opened. Recipients can choose not to allow TISL to view this information by amending "Update Preferences". Additional disclosures have been added to disclaimers included in any e-mail campaigns to highlight this. Campaign Monitor's privacy policy is available here - https://www.campaignmonitor.com/trust/privacy-hub/

TISL uses Humanitix events management software for occasional events management. This will import basic contact information (name, company, e-mail address and mobile and catering preferences). Humanitix's privacy policy is available here - https://help.humanitix.com/en/articles/8905589-privacy-and-data-security

TISL's website has allowed for voluntary online enquiries to be made (this service was discontinued in Q1 2021)

Note also that TISL's website uses Cookies. A cookie is a small data file that a website may write to your hard drive when you visit it. A cookie file can contain information, such as a user ID, that the website uses to track the pages you have visited. The only personal information a cookie can contain is information you personally supply. A cookie cannot read data off your hard disk or read cookie files created by other websites. TISL may use cookies (without further notice to you) to track user traffic patterns and to better serve you when you visit the website. You can set your browser to notify you when you receive a cookie, providing you with the opportunity to either accept or reject it. You can also refuse all cookies by turning them off in your browser, however doing so may limit your ability to use TISL's website.

7. Accuracy of personal information

TISL aims to ensure that the personal information kept is accurate, up-to-date, complete, relevant and not misleading

8. Access and correction of personal information

Clients have a right to access and seek correction of personal information that TISL holds about the client, in accordance with the Privacy Act

Where information is held in such a way that it can be readily retrieved by TISL, TISL will, on request, provide information to the client, in accordance with the Privacy Act.

TISL may recover from the client reasonable costs of supplying the client with access to personal information. However, TISL will not charge the client for the making of the request or to correct or update the personal information.

If the client would like to access or correct personal information, the client may contact TISL's Privacy Officer via the contact details listed below. TISL will respond to the request within 20 working days. TISL may decide to grant or refuse access to or correction of personal information. If TISL refuses to provide access to or correct the information, it will notify the

client of the reasons for refusal to the extent of TISL's legal obligations. TISL may also add a statement of correction to the client file that clearly shows that the individual asked to have the information changed or corrected.

9. Retention of information

TISL will not keep client information for longer than it is required for the purposes for which the information may be lawfully used. If personal information is no longer required, or for any reason authorised under NZ law, it will be destroyed.

10. Disclosing Information Overseas ("cross-border disclosure")

10.1 Due Diligence

Personal information may only be disclosed to an overseas agency if that agency has a similar level of protection to New Zealand, or the individual is fully informed and authorised the disclosure.

TISL must undertake the necessary due diligence of overseas agencies **before** making a cross-border disclosure of personal information.

TISL may only participate in a cross-border disclosure if the offshore agency meets the following criteria:

1. Is subject to the Privacy Act because the agency does business in New Zealand; or

2. Is subject to privacy laws that provide comparable safeguards to the Privacy Act, or they agree to protect the information in such a way e.g. by using model contract clauses; or

3. Is covered by a binding scheme or is subject to the privacy laws of a country prescribed by the New Zealand Government.

If none of the above criteria apply, TISL may only make a cross-border disclosure with the permission of the person concerned. The person must be expressly informed that their information may not be given the same protection as provided by the New Zealand Privacy Act.

10.2 Cloud Storage

TISL may send information to an overseas organisation to hold or process on their behalf as their 'agent'. This will not be treated as a disclosure under the Privacy Act. E.g. an overseas company providing cloud-based services for a New Zealand organisation. TISL will be responsible for ensuring that their agent – the overseas company – handles the information in accordance with the New Zealand Privacy Act

10.3 Urgent Disclosures

TISL may need to make a cross-border disclosure in certain, urgent circumstances where it would not otherwise be allowed. Information privacy principle 12 (IPP 12) allows cross-border disclosure when it is necessary to maintain public health or safety, to prevent a serious threat to someone's life or health, or for the maintenance of the law.

11. Privacy Complaints

If the client believes TISL has breached the Privacy Act or a registered code that binds TISL, the client may contact TISL's Privacy Officer via the contact details listed below. TISL may

request that the client puts the complaint in writing. TISL will endeavour to resolve the complaint in a reasonable time frame (usually within 20 working days) and may contact the client in order to obtain further details in order to provide the client with a full and complete response.

If the client is not satisfied with the manner in which TISL has handled the complaint, the client can lodge a complaint with the Office of the Privacy Commissioner at www.privacy.org.nz.

12. Breaches

If TISL has a privacy breach that has caused *serious harm* to someone (or is likely to do so), TISL must notify the Office of the Privacy Commissioner as soon as practicable. Breaches must be lodged via NotifyUs at www.privacy.org.nz.

If a notifiable privacy breach occurs, TISL should also notify any person that is affected as soon as possible after the breach occurs, unless relying on permitted exceptions set out in s116 of the Privacy Act.

When assessing whether a privacy breach is likely to cause serious harm in order to decide whether the breach is a notifiable privacy breach, TISL must consider the following:

(a) any action taken by TISL to reduce the risk of harm following the breach:
(b) whether the personal information is sensitive in nature:
(c) the nature of the harm that may be caused to affected individuals:
(d) the person or body that has obtained or may obtain personal information as a result of the breach (if known):
(e) whether the personal information is protected by a security measure:
(f) any other relevant matters.

Any privacy breaches, whether notifiable or not, will be recorded in the Breach Register (Refer to Annexure 2).

13. Criminal Offence

It is now a criminal offence (maximum fine per offence is $10,000):

- for a person to mislead TISL by impersonating someone, or pretending to act with that person's authority, to gain access to their personal information to have it altered or destroyed.

- for TISL to destroy a document containing personal information, knowing that a request has been made for that document.

14. Privacy Officer Contact Details

To access or correct personal information, to notify TISL of an alleged breach of the Privacy Act or a registered code or if there is any privacy related inquiry, please contact:

Privacy Officer
The Investment Store Limited
Suite 3, 218 Parnell Road, Parnell, Auckland 1151

Telephone No: 0800 331 041
Email: info@theinvestmentstore.co.nz

15. Board Approval

This policy has been accepted and approved by the Board.

Signature: 

Position: Director

Date: 14/03/25

Annexure 1 – Privacy Principles

Privacy Principles

- **Principle 1** - You can only collect personal information if it is for a lawful purpose and the information is necessary for that purpose. You should not require identifying information if it is not necessary for your purpose.

- **Principle 2** - You should generally collect personal information directly from the person it is about. Because that won't always be possible, you can collect it from other people in certain situations. For instance, if:
    - the person concerned gives you permission
    - collecting it in another way would not prejudice the person's interests
    - collecting the information from the person directly would undermine the purpose of collection
    - you are getting it from a publicly available source.

- **Principle 3** - When you collect personal information, you must take reasonable steps to make sure that the person knows:
    - why it's being collected
    - who will receive it
    - whether giving it is compulsory or voluntary
    - what will happen if they don't give you the information.

  Sometimes there may be good reasons for not letting a person know you are collecting their information – for example, if it would undermine the purpose of the collection, or if it's just not possible to tell them.

- **Principle 4** - You may only collect personal information in ways that are lawful, fair and not unreasonably intrusive. Take particular care when collecting personal information from children and young people.

- **Principle 5** - You must make sure that there are reasonable security safeguards in place to prevent loss, misuse or disclosure of personal information. This includes limits on employee browsing of other people's information.

- **Principle 6** - People have a right to ask you for access to their personal information. In most cases you have to promptly give them their information. Sometimes you may have good reasons to refuse access. For example, if releasing the information could:
    - endanger someone's safety
    - create a significant likelihood of serious harassment
    - prevent the detection or investigation of a crime
    - breach someone else's privacy.

- **Principle 7** - A person has a right to ask an organisation or business to correct their information if they think it is wrong. Even if you don't agree that it needs correcting, you must take reasonable steps to attach a statement of correction to the information to show the person's view.

- **Principle 8** - Before using or disclosing personal information, you must take reasonable steps to check it is accurate, complete, relevant, up to date and not misleading.

- **Principle 9** - You must not keep personal information for longer than is necessary.

- **Principle 10**- You can generally only use personal information for the purpose you collected it. You may use it in ways that are directly related to the original purpose, or you may use it another way if the person gives you permission, or in other limited circumstances.

- **Principle 11** - You may only disclose personal information in limited circumstances. For example, if:
    - disclosure is one of the purposes for which you got the information
    - the person concerned authorised the disclosure
    - the information will be used in an anonymous way
    - disclosure is necessary to avoid endangering someone's health or safety
    - disclosure is necessary to avoid a prejudice to the maintenance of the law.

- **Principle 12** - You can only send personal information to someone overseas if the information will be adequately protected. For example:
    - the receiving person is subject to the New Zealand Privacy Act because they do business in New Zealand
    - the information is going to a place with comparable privacy safeguards to New Zealand
    - the receiving person has agreed to adequately protect the information – through model contract clauses, etc.

  If there aren't adequate protections in place, you can only send personal information overseas if the individual concerned gives you express permission, unless the purpose is to uphold or enforce the law or to avoid endangering someone's health or safety.

- **Principle 13** - A unique identifier is a number or code that identifies a person in your dealings with them, such as an IRD or driver's licence number. You can only assign your own unique identifier to individuals where it is necessary for operational functions. Generally, you may not assign the same identifier as used by another organisation. If you assign a unique identifier to people, you must make sure that the risk of misuse (such as identity theft) is minimised.

Annexure 2 – Breach Register

BREACH REGISTER

Client Name	Summary of breach	Date occurred	Is it a notifiable privacy breach?	If yes, date Reported to Privacy Commissioner	Action taken to change procedures, if any.	Status (open/closed)