Privacy Policy

IS Industry Fund Pty Ltd ATF Intrust Super

Document owner: Executive Manager Risk and Company Secretary

Document approver: Board

1. Our Commitment to your Privacy

This Privacy Policy outlines how we, the Intrust Super Group[1], manage and handle the 'personal information' of our members, applicants for membership, clients, employees, applicants for employment, and other stakeholders we deal with from time to time.

'Personal Information' is any information that can identify you or that can reasonably enable your identification. 'Sensitive information' is a subset of personal information which is subject to greater security and controls, and is further defined in 'Section 3' below. In this Policy, references to 'personal information' includes 'sensitive information'. Some examples of the type of personal information we may collect about you is also included under 'Section 3' below.

The Intrust Super Group places a very high priority on the protection of your privacy and the security of your personal information and we are committed to meeting our legal obligations to comply with the Privacy Act 1988 (Cth) (the Privacy Act), which includes the Australian Privacy Principles.

As part of our commitment to protecting your privacy, we have put in place appropriate and adequate practices and procedures to manage the collection, use, disclosure and protection of your personal information in an open and transparent way.

2. Scope of this Policy

This Policy applies to the 'Intrust Super Group' which includes:

- the Intrust Super Fund (the Fund);
- IS Industry Fund Pty Ltd as trustee of the Fund (Trustee);
- IS Financial Planning Pty Ltd, a wholly owned subsidiary of the Trustee; and
- IS Investments Pty Ltd, a wholly owned subsidiary of the Trustee.

References to 'we', 'our' or 'us' throughout this Policy are references to the Intrust Super Group.

3. Types of Personal Information we collect

We collect and hold a wide variety of personal information for our business activities. The information we collect may include, but is not limited to:

i. Information about your identity, such as your name, date of birth, gender, address, residency and citizenship and/or identification documents eg driver's licence, tax file number or employment details;
ii. Information we may need to contact you eg residential or postal address, contact telephone numbers, email addresses;
iii. information about your employer, your occupation and income;
iv. information about your superannuation benefits, including associated financial information, contribution history, banking details, and similar information about your spouse, dependents or other preferred beneficiaries;
v. information about your investments;
vi. information to assist the Trustee in determining how the member's funds, including a death benefit, should be distributed if you are a potential beneficiary for a member of the Fund;

1. Refer 'Section 2.0 Scope of this Policy'

vii. any other personal information relevant to the acquisition or provision of a product or service offered by the Intrust Super Group, including sensitive information*; and

viii. , details of your employment history, resume, qualifications, training, references, psychometric testing and background checks if you are a prospective employee, in addition to the information specified in 3(i) above.

When we collect personal information from you we will provide you with a copy of or access to this Privacy Policy to ensure that you understand how we collect, use, disclose and protect your personal information.

**Sensitive information - we will only collect sensitive information with your consent. This might include information about your health, racial or ethnic origin, union memberships, sexual orientation, relationship status, criminal history, or genetic / biometric information where this is necessary for the provision of a product or service by us. An example of this is the collection of information about your health to process a claim made under an insurance policy or information about your relationship status where we need to assess your eligibility as a beneficiary for a death claim. Unless you provide your consent, or we are required by law, we will only disclose your sensitive information for the purpose for which you gave it to us or for directly related purposes you would reasonably expect.*

4. Why we collect and hold your Personal Information

We collect, hold, use and disclose your personal information where it is required for our business activities. These activities include:

i. setting up one or more superannuation benefit accounts for you;

ii. identifying you, your beneficiaries, or any other authorised representatives acting on your behalf;

iii. complying with legal requirements[2] that require or authorise us to your collect personal information e.g. collecting tax file numbers;

iv. receiving and posting contributions paid by you or for you e.g. through your employer;

v. investing your funds in line with your selected investments;

vi. providing you with income protection insurance, life insurance and/or total and permanent disability insurance, and assessing a claim for any of these insurances;

vii. collecting and assessing health/medical information for the purpose of assessing applications for insurance or claiming for a benefit/insurance provided through us;

viii. obtaining salary and income information in relation to superannuation benefits and/or insurance cover;

ix. paying superannuation benefits to you or your beneficiaries;

x. discussing your accounts with you, or providing any information about the products or services we offer;

[2] These legal requirements include, but are not limited to, the Superannuation Industry (Supervision) Act 1993 (Cth), the Superannuation (Unclaimed Money and Lost Members) Act 1999 (Cth); the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth); the Corporations Act 2001 (Cth); the Income Tax Assessment Act 1936 (Cth); the Income Tax Assessment Act 1997 (Cth); and the Insurance Contracts Act 1984 (Cth).

xi. rolling over your superannuation benefits to you, your beneficiaries, another superannuation fund, Retirement Savings Accounts, or other authorised rollover entities;

xii. processing enquiries or complying with court orders in relation to family law matters;

xiii. marketing communications or conducting marketing or product research– see Section 5 below;

xiv. assisting in locating lost superannuation accounts and re-establishing contact with lost members;

xv. investigating a complaint;

xvi. providing you with financial planning advice;

xvii. assessing suitable job candidates for career opportunities with the Fund; and

xviii. any other purpose that directly relates to why we originally collected the information from you, including data analysis, and where the use would reasonably be expected without your permission.

5. Use and disclosure of Personal Information for Marketing

We may use your personal information to send you information about superannuation, financial planning, insurance, seminars, or other products and services that we offer. We may also contact you to undertake market or product research. We use various methods to communicate with you, including mail, telephone, email, SMS or other electronic means such as through social media or targeted advertising through the Intrust Super Group or third-party websites.

If you do not want to receive marketing communications or the promotional material outlined above, we will provide a simple method by which you can opt of these communications. You can contact us at any time on 132 467 or use any of the other avenues described below in 'Section 14 How to Contact the Fund'.

The Fund will never disclose your personal information to a third party for the purposes of direct marketing unless you have given us your express consent for such disclosure and use.

6. How do we collect your Personal Information?

We collect your personal information from:

- you, or your authorised representative, directly;
- your employer e.g. your name, date of birth, contact details and superannuation contributions;
- referees, previous employers and background checking agencies where you are applying for a job with us and only with your prior consent; and
- other third parties such as medical or health professionals, other service providers, government departments, other superannuation funds, clearing houses, claims investigators, insurers or identification verification providers.

Some of your personal information may be publicly available and may be collected by us through publicly available sources eg public registers or social media.

Our Fund administration service provider, Australian Administration Services Pty Ltd (AAS) often collects this information on our behalf.

The methods used to collect your personal information are varied and include collection in person, via phone call, email, letter, fax, online, a form (electronic or hard copy), via our website (including through MemberAccess), or through a mobile device or electronic media.

Further detail on some of these methods of collection are outlined below:

Electronic Forms

We use online forms to enable you to lodge applications, update your details, change your investment, make enquiries, or provide information requested by us.

When you save or submit a form using this service it is encrypted and stored in a secure server located overseas, including countries such as Germany and/or the United States of America After we download a submitted form, it is deleted from that server.

Our Website

We operate our own website at intrust.com.au. Our website is 'cookie' free, which means we will not use information obtained from your browsing activities to send you any unsolicited information. We do however log the following information for statistical purposes:

- your server address;
- top level domain name (for example .com, .gov, .au, etc)
- the date and time of your website visit;
- the pages you looked at;
- the documents you downloaded;
- the previous site you visited; and
- the type of browser you used.

We will not try to identify users or their browsing activities except where we are legally required to do so e.g. as part of an investigation by a law enforcement agency.

Our website may contain links or references to other websites (including social media) to which this Intrust Super Group Privacy Policy does not apply. You should review the privacy policy of these websites to determine whether any personal information you disclose via these websites is adequately protected.

None of your personal information is stored or published on our website.

Member Access Portal

Our 'Member Access' portal collects browsing information from individuals who access this service. Personal Information submitted via the Member Access Portal is encrypted.

Email lists, registrations and feedback

We will collect information that you provide to us when you apply for membership, you sign up to mailing lists, where you register for an event hosted by us, or when submitting feedback to us e.g. a complaint.

We use an external service provider to manage our mailing lists and event registrations. You can access our service provider's Privacy Policy here.

Unsolicited personal information

Where we receive personal information about you which we have not requested (unsolicited information) we will assess whether we could have collected the information in accordance with this Privacy Policy and may decide to retain it for our business activities. Where we determine that we could not have solicited the information ourselves under this Policy, or we elect not to retain the information, we will take reasonable steps to destroy or de-identify the information, provided we are lawfully able to do this.

7. Disclosure of your Personal Information

We may disclose your personal information:

- where you have consented to the use or disclosure;
- within the Intrust Super Group;
- to our Fund administration service provider, AAS;
- to your employer;
- to other service providers, agents and contractors;
- to a government body or agency (in accordance with legal requirements) or where we are required to make a disclosure under the law or for law enforcement purposes (e.g. court proceedings, warrant); or
- where it is necessary to lessen or prevent a serious or imminent threat to somebody's life, health, safety or welfare.

Where you provide your personal information for the purpose of identity verification, our third-party service provider will use the Green ID verification process. Your information will be subject to an information match request in relation to relevant official record holder information and a corresponding information match result will be provided via the use of third-party systems.

Further information in relation to the some of the above disclosures is outlined below:

Service Providers, agents and contractors

We use a number of specialist service providers, agents and contractors to assist in the operation of the Fund. These include, but are not limited to:

- external service providers, including our Fund administration service provider, AAS and various information technology providers;
- web hosting companies and website developers;
- investments managers;
- legal, accounting and audit (internal and external) service providers;
- insurers; and
- recruiters or employment screening service providers (only where you have applied for a job within the Intrust Super Group).

A list of our current service providers who provide material business activities to the Fund can be found on our website at intrust.com.au.

Our providers of material business activities are appointed in accordance with our Outsourcing Policy and are subject to the Australian Privacy Principles. To further protect personal information we disclose we enter into a contract with the service provider which requires them to only use or disclose the information for the purposes of the contract and to confirm that they have appropriate mechanisms in place to maintain and enforce their own privacy policy.

Regulators or external dispute resolution

We will generally only disclose your personal information to government regulators or the Australian Financial Complaints Authority (AFCA), if you agree and where the information will assist the Fund or the regulator / AFCA to investigate a matter, or where we are otherwise legally required to disclose the information.

Overseas disclosure

Generally, we will only disclose your personal information overseas where we are required to do so for business purposes. Examples of this include:

- where you have asked us to rollover superannuation funds to a New Zealand KiwiSaver scheme we will disclose your personal information to the New Zealand scheme provider;
- if you have insurance through the Fund, your personal information may be disclosed to our insurer, their reinsurers, business partners or service providers. These entities may be located overseas;
- where IT service providers, located overseas, access our systems to provide maintenance or technical support services;
- external storage of information as described in Section 14 below.

We will take all reasonable steps to ensure that the overseas recipients of your personal information do not breach any privacy obligations under Australian laws in relation to your personal information.

8. Anonymity

Wherever possible, we will allow you to interact with us anonymously or using a pseudonym. For example, if you contact our general enquiries line 132 467 with a question you do not need to provide your name or other personal details unless we specifically require it to respond to your query. However, for many of our activities we will usually need some form of personal information to enable us to fairly and professionally handle your inquiry, request, complaint or application. If you choose to remain anonymous it is unlikely that we will be able to provide you with our products and services.

9. Quality of personal information

To ensure that the personal information we collect is accurate and up to date we take reasonable steps to:

- record information in a consistent format;
- promptly update or add new personal information to our existing records; and
- ensure that any information that we use or disclose is, having regard to the purpose of the use or disclosure, accurate, up to date and relevant.

10. Use of Government-related identifiers

We will not use or disclose a government related identifier related to you except:

- as may be necessary for us to verify your identity or conduct our business activities; or
- where the use or disclosure is required or authorised by law.

11. Storage and security of personal information

We take reasonable steps to protect the security of the personal information we hold by:

i. regularly assessing the risk of misuse, interference, loss, unauthorised access, modification or disclosure of information held by us;

ii. taking measures to address the risks identified in i. above. For example:

- we keep a record (audit trail) of when someone has added, changed or deleted personal information held in our electronic databases;
- we have policies and procedures in place which require our employees to comply with strict information security requirements; and
- we control access to our information systems through identity and access management;

iii. monitoring and reviewing our security measures and controls; and

iv. destroying or de-identifying personal information in a secure manner when we no longer need it or are no longer legally required to retain the information.

Except for information held by our insurers (which is discussed below), the majority of our records are stored electronically in a secure data server or data centre located across various sites within Australia. Some member and employer information is also stored in the cloud, which is hosted within Australia.

Our physical records are kept either in a secured office within the Intrust Super Group or its administrator, AAS, in a secure, external storage facility, or in an electronic form which is protected using appropriate security measures.

Our Death and TPD insurer, AIA Australia Ltd (AIAA) stores data on local servers within Australia.

Our Payguard insurer, Chubb Insurance Australia Limited, stores personal information both within and outside Australia. They may disclose your personal information to other entities within the Chubb group of companies such as the regional head offices of Chubb located in Singapore, UK or USA (Chubb Group of Companies), or third parties with Chubb has sub-contracted to provide a specific service, which may be located outside of Australia (such as in the Philippines or USA). These entities and their locations may change from time to time.

12. Accessing and correcting your personal information

You have the right to ask:

a. for access to any personal information that we hold about you; and

b. that we correct any of your personal information held by us if it is inaccurate, out of date, incomplete, irrelevant, misleading or otherwise incorrect having regard to the purpose for which it is held.

You can request access or correction of your personal information by contacting us via the Contact Details set out below in Section 14 How to contact Fund, or by completing a 'Change of Member Details' form to correct your personal details.

We will respond to your request within a reasonable timeframe. Unless there is a law that allows or requires us not to, we must give you access to your personal information, and take reasonable steps to correct it if we consider it is incorrect. We will require you to verify your identity and/or provide other suitable evidence before we give you access to your personal information or correct it.

We will try to make our processes around access or updating information as simple as possible. We will provide you with written reasons where we refuse to give you access to, or correct, your personal information and advise you of your options to make a complaint about our refusal. If we make a correction and we have disclosed the incorrect information to our service providers or other third parties, you may request that we advise these service providers or other parties with the updated, correct information. We will take reasonable steps to do this unless there is a valid reason not to.

If we refuse to correct your personal information, you can ask us to link a statement to your personal information indicating that you believe the information is incorrect and why.

13. How to make a complaint

If you wish to complain to us about how we have handled your personal information you should contact us on 132 467 or make a written complaint using the contact details set out below in Section 14 How to contact the Fund. If we receive a complaint from you about how we have handled your personal information we will determine what (if any) action, we should take to resolve the complaint. If we decide that a complaint should be investigated further, the complaint will be handled by our Privacy Officer or, where this is not appropriate eg due to a conflict, then a senior executive of the Fund will investigate the complaint.

We will acknowledge receipt of your complaint as soon as possible and may request further information from you that may reasonably be required to resolve your complaint. We aim to formally respond to your complaint within 30 days.

If you are not satisfied with our response or how we handled your complaint, you may complain to the Office of the Australian Information Commissioner at:

GPO Box 5218

Sydney NSW 2001

Phone: 1300 363 992

Email: enquiries@oaic.gov.au

14. How to contact the Fund

You can contact us by:

Email: info@intrust.com.au

Website: www.intrust.com.au

Telephone: 132 467

In person: Level 21, 10 Eagle St, Brisbane, Qld 4000

Post: GPO Box 1416 Brisbane QLD 4001

Facsimile: 1300 663 844

15. Updates and Availability of this Privacy Policy

This Privacy Policy must be made publicly available on the Intrust Super website at intrustsuper.com.au.

You may request a copy of this Privacy Policy be sent to you, free of charge, by contacting us at 132 467 or emailing us at info@intrust.com.au.

From time to time we may update this Privacy Policy to reflect changes in our information handling practices. These updates will be published on our website, intrust.com.au.

This Privacy Policy is effective from 28 September 2019.