Privacy Policy

This document outlines the policy of Australian Super Manager Pty Ltd with respect to handling the personal information we collect.

Australian Super Manager Pty Ltd (ASM) provides Self Managed Superannuation Fund (SMSF) administration to superannuation fund trustees. Our work is often in conjunction with your personal professional advisers.

'ASM', 'we', 'us' or 'our' refers to the Australian Super Manager Pty Ltd.

We will act to protect your personal information in accordance with the Australian Privacy Principles (APP). We only collect the personal information we reasonably require, in the course of our business of providing services, in accordance with this Privacy Policy by lawful, fair, and non-intrusive means. We cooperate with police and other enforcement and regulatory bodies as required or allowed by law.

We collect personal information to provide you with the products and services you request as well as to provide information on other products and services offered by or through us. The law requires us to collect and retain personal information. Personal information may be used and disclosed within the Group to administer our products and services, and, unless you tell us otherwise, to provide you with related marketing information.

You can seek access to the personal information we hold about you. If the information we hold about you is inaccurate, incomplete, or outdated, please let us know so that we can correct it (our contact details are provided at the end of this document).

COLLECTION, USE & DISCLOSURE OF YOUR PERSONAL INFORMATION

What personal information do we collect and hold?

Personal information is information or opinion that allows others to identify you. It includes your name, age, gender and contact details. The kinds of personal information we collect and store will depend on what products and services you request from us. However, our ability to provide you with services and advice that meets your needs and objectives may entail us collecting information, including:

- your contact details including names, address, phone, and email address;
- details of your financial needs and objectives;
- personal details including your date of birth, associated entities, visa and residency status;
- details of your occupation, marital status, financial dependants, and identification details such as copies of birth certificate or drivers' licence or other documentation;
- details of your current financial circumstances, including your assets and liabilities (both actual and potential), income, expenditure, personal insurance cover, general insurance, superannuation, taxation, and credit reports - where appropriate;
- details of your investment preferences, experience and aversion or tolerance to risk;
- details of any professional advisers you engage with;
- estate planning details;
- details of agents or affiliates including, but not limited to, a guardian, carer or a person acting on your behalf as an attorney;
- information about your employer, your employment history including future, family commitments including dependents and social security eligibility;
- your tax file number;
- personal and family medical history;
- your agreement to grant access to a spouse or partner's information.

What sensitive information do we collect and hold?

Sometimes we may collect sensitive information about you. This could include information on:

- your race or ethnic origin;
- your political opinions or membership of a political organisation;
- your religious beliefs and affiliations;
- your philosophical beliefs;
- your membership of a professional association or trade union;
- your sexual preferences and orientation;
- genetic information; and
- biometric information or templates.

We will collect, maintain, use, and disclose personal information which is necessary for us to adequately provide the services you have requested including:

- Bookkeeping services
- Preparation of minutes and record management
- Preparation of Financial Statements
- Taxation Services
- Provision of Member Statements and Centrelink/DVA schedules
- Liaising with Financial Advisor and other professional financial services
- Coordination of Audit Services
- Providing estate planning support

As well as providing us with information upon which to provide a customised solution to your needs and objectives, we are required under the Corporations Act 2001 (Cth) and the National Consumer Credit Protection Act 2009 (Cth) to collect and hold this information.

How we collect information

Generally, we will not collect personal information about you except when you have knowingly provided that information to us or have authorised a third party to provide that information to us. Sometimes we collect information about you from other sources. We may collect information about you that is publicly available (for example from public registers or social media). The majority of information collected by us will be provided by way of your completion of a financial fact find or via your professional adviser/s.

We may seek your express permission to collect information from other entities such as product providers, accountants, solicitors, etc where this information may not be currently available to you. If we were to obtain information that is not information that could have been provided or authorized for collection by you, we will de-identify and destroy this information unless it is unlawful to do so.

Identification documentation may be required for collection by law under the Anti-Money Laundering and Counter Terrorism Financing Act 2006 (Cth),. In some instances, we are required to verify this documentation against other records. For instance, identification for Australian companies, trusts or registered co-operatives may need to be verified by a search of records held by regulatory bodies such as Australian Securities and Investments Commission (ASIC) or the Australian Taxation Office (ATO) etc.

Use of information

We will not use or disclose personal information collected by us for any purpose other than:

- the purposes for which it was provided or secondary related purposes in circumstances where you would reasonably expect such use or disclosure; or
- where you have consented to such disclosure; or

- where the APP authorise use or disclosure where required or authorised under law, in circumstances relating to public health and safety and in connection with certain operations by, or on behalf of, an enforcement agency or regulatory body.

We are obliged to maintain records which include personal information and make those records available for inspection by [the] ASIC or other regulators under a relevant law. If we provide information for the purpose of law enforcement activities, we will make a record of that provision.

It is a condition of our agreements with each of our authorised representatives (both personal and corporate) that they adopt and adhere to this Privacy Policy. You can be assured that all authorised representatives and their staff (agents) will use your information in accordance with this policy. If you have any concerns in this regard, you should contact us by any of the methods detailed in this document.

If you chose not to provide your information

The effectiveness of our services is specifically dependent on information you provide and it being relevant, complete, accurate and up to date. Without this, our services may not meet your needs or may result in unforeseen financial consequences. If you elect not to provide us with your personal information, as and when requested, we may not be able to provide you with services.

Marketing

We may use personal information collected from you for the purpose of providing you with direct marketing material; however, if you do not wish to receive such information you can request not to receive it. Simply contact us by any of the methods detailed in this document. There is no cost for this request, however, please allow two weeks for your request to be actioned.

ASM adheres to the Spam Act 2003 (Cth), accordingly, we will:

- obtain your consent before sending an electronic message to you (this can be express or inferred);
- provide sender identification (so that you know who sent the message); and
- provide you with the option to unsubscribe.

Disclosing information to other parties

In order to provide our services, we may disclose your personal information to external parties, including, but not limited to:

- affiliated product and service providers as well as external service providers such as superannuation fund trustees, insurance providers, and product issuers for whom we act as agent (so that they may provide you with the product or service that you seek or in which you have an express interest);
- auditors we appoint to ensure the integrity of our operations;
- suppliers from whom we order goods and services on your behalf (so that those goods and services can be provided to you);
- other persons acting on your behalf including your financial adviser, accountant, solicitor, executor, administrator, trustee, guardian, or attorney;
- if required or authorised to do so under law, law enforcement agencies, regulatory bodies, and government organisations;
- medical assessment services where you have sought insurance for the purposes of underwriting an insurance policy;
- other organisations, who, in conjunction with us, provide their products and services (so that they may provide their products and services to you); and
- potential owners, under a confidentiality agreements, if we decide to sell all or part of the business. In the event that a sale of our business is affected, we may transfer your personal information to the purchaser of the business. As a client you will be advised of any such transfer and your information will not be exchanged if you object to the transfer.

If we have used an example to describe when we might exchange personal information, the exchange of personal information may not be limited to those examples or examples of a similar kind.

We disclose personal information when we outsource certain functions, bulk information overseas allow access to relevant personal information for external organisations that help us provide services. These organisations are bound by confidentiality arrangements. From time to time we may use service providers whose staff accesses our data outside of Australia to provide services. Where this is the case, these service providers have committed to adhere to the Australia Privacy Principles. These service providers may be located in a number of countries including India.

In all circumstances where personal information may become known to our contractors, agents, AFSLs, authorised representatives or their agents and outsourced service providers, there are confidentiality arrangements in place. Contractors, agents, AFSLs, authorised representatives or their agents and outsourced service providers are not able to use or disclose personal information for any purposes other than our own. The Group takes its obligations to protect client information very seriously and we make every effort to deal only with parties who share and demonstrate the same attitude. If we have used an example to describe when we might exchange personal information, the exchange of personal information may not be limited to those examples or examples of a similar kind.

Sending personal information overseas

We take reasonable steps to ensure that overseas recipients adhere to the APP. We may disclose your personal information to contractors overseas to provide services to you; however, when doing so you should be aware of the following:

- your personal information may be accessed by staff, representatives, or agents in other countries, if that becomes necessary to deliver our services to you. This access is via secure internet connection or in some instances by email;
- from time to time, information may be loaded to the cloud for storage or access through programs such as SharePoint etc; and
- it is possible that product and services providers we recommend may outsource functions using overseas contractors or companies that process these services using offshore resources. Where this is a concern to you, we suggest that you carefully read their Privacy Policy to determine the extent to which they send overseas.

Website, Social Media and Email

When you visit our website, details such as time and date, your computer IP address, pages accessed, time spent on page and type of browser, may be recorded about your visit. If you provide information on a social media platform, including, but not limited to, LinkedIn, Facebook, Twitter, and Instagram, we may hold, store, and disclose this information for the purposes of marketing or the provision of services to you. This information is used in an anonymous format for statistical purposes and as such cannot identify you individually, unless we have sought permission from you to do so. If you do not wish this to happen, please notify us.

When you log into the client section of our site, we may use cookies to identify who you are, while you are logged in for the session. The cookie is unique to that session, and the data within the cookie is encrypted. You must have cookies enabled to be able to use our site. Our website may contain links to other websites. When visiting these websites be sure to check the Privacy Policy as we are not responsible for privacy practices of those other parties. Where you chose to communicate with us by email, we will store your email, name and address with any other contact or personal details you have provided on our database.

Government Related Identifiers

We will not adopt as our own any identifiers that you may provide to us such as TFNs, Centrelink, Medicare numbers etc. If you have provided us signed consent, we may hold your identifiers on file so that we can provide ongoing services to you. If you chose not to provide this consent, we will not hold this information on file. The circumstances in which an organisation may use or disclose government related identifiers are narrower in scope than the circumstances in which an organisation may use or disclose other personal information. Government related identifiers will not be disclosed except in the following circumstances:

- where use or disclosure is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions;
- to verify that an individual is who or what they claim to be, for example, to verify their name or age;
- to fulfil our obligations to an agency or a State or Territory authority;
- as required or authorised by or under an Australian law or a court/tribunal order;

- where use or disclosure may lessen or prevent a serious threat to life, health, or safety;
- when taking appropriate action in relation to suspected unlawful activity or serious misconduct;
- when disclosure of a government related identifier to an enforcement body is requested for enforcement related activities; and
- as prescribed by regulations.

Accessing and Correcting your Information

Our goal is to ensure that the personal information we hold about you is accurate, secure, complete and up to date. Please contact us if you believe that the information, we have about you is not complete, accurate or up to date. You can ask us to update or change information in your file at any time. Prior to providing this access we will require you to provide evidence of your identity. We may ask you to put your request in writing and any charge we make for providing access will be reasonable. We may take steps to update information, for example, an account balance from your account service provider where you have provided us with access rights or an address or contact number from publicly available information such as telephone directories or websites.

If you ask, we will tell you what personal information we hold about you within your client file and what we do with it. On receipt of your request, we will, subject to the limitations outlined below, facilitate access to you by allowing an inspection of your client file in person, or by providing copies or an accurate summary of relevant documents, depending on what we believe is most appropriate in the circumstances.

If for whatever reason we refuse to change information we hold on your file, we will arrange for a statement from you to be associated with the relevant information so that it can be included in any future use or disclose of that information should you wish to do so.

When we make reference to your client file we are referring to documents, including, but not limited to: data collection forms; written communications (such as letters and emails) from you to ASM, and from ASM to you (or your professional advisers); Statements of Advice (SoAs), Records of Advice (RoAs); tax returns and correspondence; transaction reports; signed authorities; investment reports, superannuation and personal insurance statements or statements produced by the issuers of financial products, and fee invoices.

In accordance with the APP, we will not provide you with access to your personal information if:

- providing access would pose a serious threat to the life or health of a person or the health and safety of the public;
- providing access would have an unreasonable impact on the privacy of others
- the request for access is frivolous or vexatious;
- the information related to existing or anticipated legal proceedings between us and would not be discoverable in those proceedings;
- providing access would reveal our intentions in relation to negotiations with you in such a way as to prejudice those negotiations;
- providing access would be unlawful;
- denying access is required or authorised by or under Australian law or by court/tribunal order;
- ASM has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to its functions or activities has been, is being, or may be engaged in, and giving access would be likely to prejudice the taking of appropriate action in relation to the matter;
- providing access is likely to prejudice actions being conducted by an enforcement agency; or
- providing access would reveal evaluative information generated within ASM in conjunction with a commercially sensitive decision-making process. In the event we refuse your request to access to your personal information; we will provide you with a written explanation for that refusal. We will endeavour to respond to any request for access within 14-30 days depending on the complexity of the information and/or the request. If your request is urgent please indicate this clearly.

Keeping your Information Secure

Your personal information is generally held in your client file and on our computer database. We will always seek to ensure that your personal information is protected from misuse, loss, unauthorised access, modification, or disclosure. At all times your personal information is treated as confidential and any sensitive information is treated as highly confidential.

Our security measures include, but are not limited to:

- educating our staff as to their obligations with regard to your personal information;
- all hard copy files are stored in lockable cabinets/rooms;
- access to our premises is controlled by only allowing authorised personnel to access those locations where personal information is stored;
- all computer-based information is protected through the use of access passwords on each computer and screen saver passwords;
- client data is backed up each evening and stored securely off site;
- encrypting data sent from your computer to our systems during internet transactions, and customer access codes transmitted across networks;
- employing firewalls, intrusion detection systems and virus scanning tools to protect against unauthorised persons and viruses from entering our systems;
- using dedicated secure networks or encryption when we transmit electronic data for purposes of outsourcing; and
- providing secure storage for physical records.

In the event you cease to be a client of this organisation, any personal information which we hold about you will be maintained in our secure storage facility for a period of 7 years in order to comply with legislative requirements. Where information we hold is identified as no longer needed for any purpose, we ensure it is effectively and securely destroyed.

Contact Us

If you seek any further information from Australian Super Manager about our Privacy Policy, please contact our Privacy Officer:

Email: info@supermanager.com.au
Address: Suite 113 24 Gordon Street Coffs Harbour NSW 2450
Postal: PO Box 1999 Coffs Harbour NSW 2450
Telephone: 1300 130 622

How to Complain

We understand that even with the best intentions of our organisation, it is possible that our actions may not meet your expectations. If you have a complaint about privacy please tell us, as we'd like the chance to fix the problem. We offer a free complaints resolution process for all our clients.

So that we are able to assist promptly, we ask you to follow the process outlined below:

- gather all the supporting documents/information relating to the complaint (we would like to hear about your specific questions and/or what you want us to do to rectify the matter); and
- contact our Privacy Officer; your situation will be reviewed, and, if possible, resolved straight away.
- If the matter has not been resolved to your satisfaction, we will provide you with the contact details of the person who will investigate your complaint, answer your questions, and do all they can to regain your confidence. We aim to resolve complaints as soon as possible. We will endeavour to provide our response within a maximum of 45 days; should it take longer we will seek your agreement to extend the timeframe.

The information in this document is considered to be true and correct at the date of publication. Changes to circumstances after the time of publication may impact on the accuracy of the information held.

Australian Super Manager Pty Ltd
ABN 34 146 029 521
Suite 113, 24 Gordon Street COFFS HARBOUR NSW 2450
Phone: 1300 130 622

Version: October 2023