Privacy policy

Our commitment

Professional Wealth Services Pty Limited (PWS) is committed to providing you with the highest levels of client service. We recognise that your privacy is very important to you. The Privacy Amendment (Enhancing Privacy Protection) Act sets out the Australian Privacy Principles (APPs). Our aim is to both support and ensure that we comply with these principles. Further information on privacy in Australia may be obtained by visiting the website of the Office of the Australian Information Commissioner at www.oaic.gov.au.

This Privacy Policy discloses how the personal information you provide to us and our representatives is collected, used, held, disclosed and disseminated.

PWS is required to meet particular legislative and regulatory requirements. In order to provide comprehensive financial planning advice to you, we are required to collect certain personal information from you.

Your personal information

As a financial planning organisation we are subject to certain legislative and regulatory requirements which require us to obtain personal information about you, in accordance with s961B of the Corporations Act, which may include, but is not limited to:

- your name, date of birth, current addresses, telephone, mobile, fax numbers, email address
- information regarding your dependants and family commitments
- your occupation, employment history and details, social security eligibility
- your financial needs and objectives
- your assets and liabilities (current and future), income, expenses
- your superannuation and insurance details
- your social security entitlements, and
- your risk profile details

We are required to also collect certain information about you for the purpose of reporting to AUSTRAC under the Anti-Money Laundering and Counter Terrorism Financing Act 2006. This information will be held securely on your file and may only be divulged to others if required under the law.

How we collect personal information

PWS collects personal information in a number of ways, including:

- directly from you, when you attend a face-to-face interview
- directly from you, when you provide information through a client data form
- directly from you, when you provide information by phone
- directly from you via email or the internet, and
- directly from fund managers, superannuation funds, life insurance companies and other product issuers once authorisation has been provided by you. You have a right to refuse us authorisation to collect information from a third party.

How we use your personal information

Primarily, your personal information is used in order to provide comprehensive and/or scoped financial planning services to you. We may also use the information that is related to the primary purpose and it is reasonable for you to expect the information to be disclosed.

Should you choose not to provide certain personal information or provide incorrect information, the advice and/or recommendations may be inappropriate or inadequate.

From time to time, we may provide you with direct marketing material. This will include articles and news-letters that may be of interest to you. If, at any time, you do not wish to receive this information any more, you may contact us with this request. We will try to meet your request within two weeks. We maintain a register for those individuals not wishing to receive direct marketing material.

We may disclose your personal information to superannuation fund trustees, insurance providers, product issuers and other service providers for the purpose of giving effect to your Statement of Advice and the recommendations made by us.

If we propose to sell the business, we may disclose your personal information to potential purchasers for the purpose of them conducting due diligence investigations. Disclosure will be made in confidence and it will be a condition of that disclosure that no personal information will be used or disclosed by them.

We do not usually collect unsolicited personal information. If we receive such information, we will determine whether or not it would have been permissible to collect that information if it had been solicited. If we determine that collection would not have been permissible, to the extent permitted by law, we will destroy or de-identify that personal information as soon as practicable.

When we disclose your personal information

In certain circumstances we are required to collect government identifiers such as your tax file number, Medicare number or pension card number, however we do not use or disclose this information other than when required or authorised by law or unless you have

voluntarily consented to disclose this information to any third party.

The Corporations Act has provided the Australian Securities and Investments Commission with the authority to inspect certain personal information that is kept on our files about you.

For the purposes set out above, we may disclose your personal information to organisations outside PWS. The organisations to which we disclose information may include:

- superannuation fund trustees, insurance providers, fund managers and other product providers in order to implement your financial plan/recommendations
- compliance consultants to ensure that our representatives are meeting our compliance standards
- temporary staff to handle workloads during peak periods
- mailing houses
- your professional advisers, including your solicitor or accountant as authorised by you
- information technology service providers to manage our IT systems
- government and regulatory authorities and other organisations, as required or authorised by law
- another authorised representative of PWS if necessary
- a potential purchaser/organisation involved in the proposed sale of our business for the purpose of due diligence, and
- a new owner of our business that will require the transfer of your personal information.

We are required under the Rules of Professional Conduct of the Financial Advice Association Australia (FAAA) to make certain information available for inspection by the Association on request to ensure ongoing compliance with mandatory professional standards. This may involve the disclosure of your personal information.

In addition, our employees and the outsourcing companies/contractors are obliged to respect the confidentiality of any personal information held by PWS.

How we store and secure this information

We keep your personal information in your client file. These files are accessible to authorised personnel only and are appropriately secured out of hours.

Your personal information may also be held on our computer database. All computer-based information is protected through the use of access passwords. Data is backed up regularly and stored securely off-site in Australia. As we also store client personal information using third party provider software, this may be stored on servers hosted outside of Australia.

Personal information will be treated as confidential information and sensitive information will be treated as highly confidential. Sensitive information includes information (or an opinion) about someone's health, religious, political or philosophical beliefs, sexual preferences, criminal record or membership of political, trade union, professional or trade associations. Sensitive information will only be collected at the initial application where insurance cover is applicable.

It is a legislative requirement that we keep all personal information and records for a period of 7 years. Should information be no longer needed after this period then we will destroy it or put the information beyond use or access.

Ensure your personal information is correct

PWS takes all reasonable precautions to ensure that the personal information we collect, use and disclose is accurate, complete and up to date. To ensure we can maintain this level of accuracy and completeness, we recommend that you:

- inform us of any errors in your personal information as soon as possible, and
- update us with any changes to your personal information as soon as possible

Access to your personal information

You have a right to access your personal information, subject to certain exceptions allowed by law. We ask that you provide your request for access in writing (for security reasons) and we will provide you with access to that personal information. Access to the requested personal information may include:

- providing you with copies
- providing you with the opportunity for inspection, or
- providing you with a summary

If charges are applicable in providing access to you, we will disclose these charges to you prior to providing you with the information.

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
- providing access would have an unreasonable impact on the privacy of others
- the request for access is frivolous
- the information is 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 law, or
- providing access would be likely to prejudice certain operations by or on behalf of an enforcement body or

an enforcement body requests that access not be provided on the grounds of national security

Should we refuse you access to your personal information, we will provide you with a written explanation for that refusal.

Anonymity and pseudonymity

You may wish to deal with us anonymously, however, this is likely to limit the services we provide to you as our principal business relates to the provision of financial services (and in most cases, the provision of personal advice) which would require individuals to provide personal information. We are also required under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) to conduct customer due diligence and appropriately identify clients.

Sending data overseas

If we transfer personal information outside Australia to our service providers or other third parties who operate or hold data outside Australia, we comply with trans-border data flow privacy standards under the Privacy Act 1988 (Privacy Act), for example, by taking reasonable steps to protect the information from being held, used or disclosed by the recipient inconsistently with the Australian Privacy Principles (Privacy Principles).

We have an outsourced provider arrangement for paraplanning where your information may be sent to Sri Lanka and/or the Philippines.

The AI and AI Systems we use store data in the Asia-Pacific (APAC) region and Australia. Data is encrypted both in transit and at rest. The data centres comply with industry standards for physical and digital security, including ISO/IEC 27001 certification.

Complaints resolutions

Please contact our Privacy Officer if you wish to complain about any breach or potential breach of your privacy rights. Your complaint will be responded to within 7 days. If you are not satisfied with the outcome of your complaint, you are entitled to contact the Office of the Australian Information Commissioner.

Our website

The PWS website provides links to third party websites. The use of your information by these third party sites is not within the control of PWS and we cannot accept responsibility for the conduct of these organisations.

You may register with us to receive newsletters and other information. By doing so, your name and email address will be collected and stored on our database.

If you do not wish to receive any further information from us, or you wish to update your registration details, please email your request to us. We will try to meet your request within two weeks.

Our website uses cookies to provide you with a better user experience. Cookies also allow us to identify your browser while you are using our site – they do not identify you. If you do not wish to receive cookies, you can instruct your web browser to refuse them.

We encourage you to check our website regularly for any updates to our Privacy Policy.

Data breach

A data breach occurs when personal information held by us is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference. Examples of a data breach are when a device containing personal information of clients is lost or stolen, or when a database containing personal information is hacked or if we mistakenly provide personal information to the wrong person.

Under the Privacy Amendment (Notifiable Data Breaches) Act 2017, we have an obligation to assess within 30 days whether a data breach amounts to an 'eligible data breach' if we become aware that there are reasonable grounds to suspect that a data breach may have occurred.

If we form the view that the data breach would likely result in serious harm to any of the individuals to whom the information relates despite any remedial action taken by us, then the data breach will constitute an 'eligible data breach'. If an eligible data breach occurs, we have an obligation to notify you and the Office of the Australian Information Commissioner and of the details of the eligible data breach.

Contact details

You may wish to contact us for the following:

- find out what personal information we hold about you;
- update or correct the personal information we hold about you;
- opt out of receiving direct marketing material
- make a privacy related complaint.

Should you wish to do so, please contact us on the details below:

Professional Wealth Services (PWS)
1300 001 312 or admin@pws.net.au
PO Box 1815 North Sydney NSW 2059
www.pws.net.au