

Privacy Policy

Sherlock Wealth Advisory Services Pty Ltd | AFSL 558532 | Version 4.0

PRIVACY POLICY

Sherlock Wealth Advisory Services Pty Ltd | AFSL 558532 | Version 4.0

Version 4.0 | 10 November 2026

Why we collect and use personal information 2

What personal information we collect 2

Accessing and correcting personal information 5

Who we share personal information with 5

Disclosure of personal information overseas 6

How we protect personal information 6

Using our website 7

Decisions made by computer programs 7

Complaints about privacy 8

About this Policy 9



We understand that the privacy of your information is important to you, and we respect the confidentiality of the information that you provide to us. Protecting your information is an important part of maintaining trust between us and our clients and by handling information in a secure manner we build strong business relationships.

This Privacy Policy (Policy) explains how we collect, hold, use and disclose personal information. It also explains how our authorised representatives may handle personal information when providing services on our behalf.

We are bound by the *Privacy Act 1988* (Cth) (Privacy Act) and the Australian Privacy Principles (APPs).

Why we collect and use personal information

We collect, hold, use and disclose personal information so we can provide you with financial products, advice and services relevant to your needs. We may also collect, use and disclose your information for related purposes such as:

- Complying with our legal obligations, such as verifying your identity
- Assisting with your questions and complaints
- Arranging for services to be provided by third parties
- Internal operations, such as record keeping, data analytics, auditing or training
- Promotion of other products and services that may be of relevance to you
- Administer and manage our relationship with you;
- Monitor and supervise our representatives;
- Undertake audits, quality assurance, risk management, compliance, remediation and training;
- Prevent, detect and respond to fraud, scams, cybersecurity incidents and other unlawful activity;
- Maintain and improve our systems, products and services; and

We may use or disclose personal information to communicate with you about products and services that may be relevant to you where permitted by law. You may opt out of direct marketing communications at any time by using the unsubscribe facility in the communication or by contacting us using the details in this Policy. We will process your request within a reasonable period and at no cost.

Opting out of direct marketing will not prevent us from communicating with you about products or services you receive from us or where we are otherwise required or authorised to contact you.

We also collect, hold, use and disclose personal information about our employees, officers, job applicants, financial advisers, contractors, service providers and other people with whom we do business. We use this information to administer and manage our business operations, relationships and legal and regulatory obligations.

What personal information we collect

We ask you for personal information that is necessary to assist us in providing relevant products and services to you for our functions and activities or where the collection is required or authorised by law. The information we collect could include (but is not limited to):

- your name, date and place of birth;
- contact details;
- identity verification information;
- financial, taxation, superannuation and insurance information;
- employment, occupation and income information;
- information about your financial circumstances, needs, objectives and preferences;
- beneficial ownership and control information;
- residency and citizenship information;
- information about your use of our products, services, systems and websites;
- records of our communications and interactions with you; and
- information required to comply with our legal and regulatory obligations.

Where relevant to the products or services being provided, we may also collect personal information about your family members, beneficiaries, business associates, representatives and other related persons.

We may collect sensitive information where it is reasonably necessary for our functions or activities and you have consented to the collection, or where the collection is otherwise required or authorised by law. For example, we may collect health, medical and lifestyle information when providing financial advice or assisting with applications relating to life insurance products.

We may also collect sensitive information where required or authorised for identity verification, customer due diligence, risk assessment, sanctions screening, fraud prevention or compliance with our anti-money laundering and counter-terrorism financing obligations. Depending on the circumstances, this may include criminal record information.

Government-related identifiers

We only adopt, use or disclose government-related identifiers where permitted by law.

Government-related identifiers we may collect include Tax File Numbers, Medicare numbers, passport numbers and driver licence numbers. We may disclose these identifiers to government agencies, superannuation trustees, financial product issuers and other organisations where permitted by law and reasonably necessary to provide products or services or comply with our obligations.

We take reasonable steps to protect government-related identifiers and to destroy or de-identify them when we are no longer required or authorised to retain them.

Identity verification information

Where we are required to verify your identity, we may collect identification information and copies of identification documents, such as passports and driver licences.

We only retain copies of identification documents where reasonably necessary or where required or authorised by law. Where identity records are subject to a statutory record-keeping requirement, we retain them for the applicable period.

Our approach to disposing of identification information and documents is explained under “How we protect personal information”.

How we collect personal information

We usually collect personal information directly from you, including when you:

- complete an application, identification form, fact find, questionnaire, risk profile or onboarding document;
- provide documents or instructions to us;
- use a client portal, secure exchange platform, website or online tool;
- apply for or use a product or service;
- make an enquiry or complaint;
- communicate with us in person, by telephone, email, online or through another electronic channel;
- participate in a survey, feedback request or client satisfaction program; or
- attend a seminar, webinar, training session or other event.

We may also collect personal information from other people or organisations, including:

- financial advisers, mortgage brokers, credit representatives and accountants;
- your authorised representatives and other professionals acting on your behalf;
- family members, employers and other persons connected with an application or service;
- financial product issuers, superannuation funds, insurers, lenders and service providers;
- medical and other health professionals;
- credit reporting bodies;
- identity verification, fraud prevention, sanctions, politically exposed person and adverse media screening providers;
- government departments, government agencies, regulators, law enforcement bodies and international organisations;
- publicly available records, websites and social media; and
- other organisations that jointly provide products or services with us.

If you don't provide information

You are not generally required to provide personal information to us. However, we may need particular information to provide products or services, assess an application, verify your identity, respond to your request or complaint, or comply with our legal and regulatory obligations.

If you do not provide the requested information, we will explain the likely consequences where practicable. Depending on the circumstances, we may be unable to:

- provide or continue to provide a product, advice or service;
- assess your application, needs or eligibility;
- process a transaction or instruction;
- verify your identity or comply with our legal and regulatory obligations; or
- respond to an enquiry or complaint.

When we may ask for your consent

In some circumstances, we need your consent before we collect, use or disclose your personal information. For example, we will generally seek your consent before collecting sensitive information, unless the collection is otherwise permitted or required by law. We may also seek your consent to use or disclose your personal information for a purpose that is different from the purpose for which it was originally collected.

When we rely on your consent, we will seek it in a manner appropriate to the circumstances.

You may withdraw your consent at any time, subject to applicable legal, regulatory or contractual requirements. Withdrawing consent may affect our ability to provide certain products or services to you.

Dealing with us anonymously

Where practicable, you may deal with us anonymously or by using a pseudonym. However, we may need to identify you where required or authorised by law or where it is not practicable to provide the requested product or service without confirming your identity.

For example, we will generally need to identify you before providing personal financial advice, credit assistance, tax agent services or financial products.

Accessing and correcting personal information

You, or someone that you nominate, can request access to personal information we hold about you. We will deal with requests for access to your personal information as soon as possible and aim to respond within 30 days. The time we require will depend on the type of information requested and whether it is in physical or electronic format. There may be a cost involved with locating, copying or sending you the information you request. The cost will be discussed and agreed with you at the time.

In some circumstances, we may refuse to provide access where an exception under the Privacy Act applies. If we refuse access, we will generally provide written reasons and information about how you may complain about the refusal, as required by law.

We take reasonable steps to ensure that your personal information is accurate, up to date and complete and relevant. We will update your personal information if you contact us. In most cases, you can update your personal information over the phone, by contacting your adviser.

You may also contact us to withdraw consent where we rely on your consent, or if you have concerns about how we handle or retain your personal information.

We may be required to retain information under the *Privacy Act*, *Corporations Act 2001* (Cth), AML/CTF legislation, taxation legislation or other applicable laws.

Who we share personal information with

We may disclose your information to a third party where you have given your consent or where you would reasonably expect us to disclose your information to that third party.

From time to time, we may share your personal information with other entities both within and outside of the Licensee. This will vary according to the product or service involved, but could include:

- any person acting on your behalf, including your financial adviser, solicitor, accountant, executor, administrator, trustee, guardian or attorney
- financial product and service providers, including financial planning software providers and paraplanners
- for corporate superannuation members, your employer or your employer's financial adviser
- other organisations within the Licensee including related bodies corporate and advice firms we have authorised,
- medical practitioners and health service providers, such as pathology services
- companies involved in the payments system including financial institutions, merchants and payment organisations
- organisations who assist us with certain business functions, such as auditors, compliance consultants, direct marketing, debt recovery and information and communication technology support
- our solicitors, our insurers, courts, tribunals and dispute resolution organisations
- other organisations who provide us with products and services so that they may provide their products and services to you or contact you on our behalf, and/or
- anyone to whom we, or our service providers, are required or authorised by law to disclose your personal information to (for example, law enforcement agencies, Australian and international government and regulatory authorities).

We may also disclose the personal information we hold about our financial advisers to professional organisations, companies and consultants that we work with. Some recipients may be located outside Australia. Further information is provided under "Disclosure of personal information overseas".

Disclosure of personal information overseas

We may disclose your personal information to service providers who operate outside Australia including Southeast Asia and Southeast Europe. The most common example of when we share your personal information overseas is:

- advice preparation and administrative support;
- cloud hosting and data storage;
- information technology and cybersecurity services;
- artificial intelligence and data analytics solutions;
- identity verification and AML/CTF screening; and
- other operational and technology services.

When we send your personal information to overseas recipients, we make sure appropriate data handling and security arrangements are in place

Your adviser may have their own outsourcing arrangements to countries other than those detailed above. If so, your adviser will disclose these arrangements separately to you. All reasonable steps will be taken to ensure that offshore service providers comply with the Privacy Act. Where applicable, you can contact the relevant representative for information about their arrangements.

How we protect personal information

We strive to ensure that the personal information that you provide to us is stored safely and securely. We take precautions to protect the personal information we hold about you from misuse, interference and loss, and from unauthorised access, modification or disclosure.

We have a range of practices and policies in place to protect personal information we hold, including:

- educating our staff and representatives about how to protect your personal information and updating them about cybersecurity developments, threats and scams,
- secure passwords in accordance with stringent password management policies
- use of Multi-Factor Authentication (MFA)
- using secure client portals and/or password protection
- strict confidentiality arrangements restricting third parties' use or disclose of personal information for any unauthorised purposes,
- data and cyber security assessments of third-party providers and systems
- employing firewalls, intrusion prevention systems web/email filtering and antivirus/antimalware tools
- a Cybersecurity Policy, Cyber Incident Response Plan, Data Breach Response Plan

We require our employees and representatives to comply with applicable privacy, confidentiality and information security requirements and undertake risk-based assessments of representatives and service providers that handle personal information.

Where personal information is no longer required, we take steps to de-identify or destroy the information in a secure manner.

If a data breach occurs, we will assess whether notification is required under the Notifiable Data Breaches scheme in the Privacy Act. Where required by that scheme, we will notify the Office of the Australian Information Commissioner and individuals at risk of serious harm as soon as practicable. Our notification will explain the breach, the kinds of personal information involved, how to contact us and the steps we recommend individuals take in response.

Using our website

Some personal information may be collected whilst navigating through and interacting with the content of our websites. The electronic methods of collection we use include cookies, log files and web beacons. The information we collect by these electronic means is generally not stored for long – they are temporary records – and can include device-specific data or log data such as your IP address, device screen size, device type, browser information, referring domain, pages visited, the date and time website pages were visited, and geographic location (country only).

We use this information to:

- operate and secure our websites and online services;
- manage access and authentication;
- understand how our websites and services are used;
- identify and resolve technical issues;
- improve website functionality and user experience; and
- provide relevant communications or content where permitted by law.

Cookies record information about your visit to our websites and it is used to improve your website experience, to serve you with relevant information and to manage your access to certain parts of our websites. You can choose if and how a cookie will be accepted by changing your browser settings; but please be aware that this may affect your access to some parts of our websites.

Web beacons help us better manage content on our websites by allowing us to understand usage patterns, fix issues, and improve the products and services offered to you on our websites. Log files contain information about the devices and browsers used to access our websites and help us to diagnose problems, analyse trends, administer the site or mobile application.

Decisions made by computer programs

[Please review and delete or amend as applicable] We use computer programs that process your personal information to help us and our representatives make decisions that could significantly affect your rights or interests. These include software, apps and tools including those that use artificial intelligence or machine learning, such as chatbots, AI assistants and agents. They may apply rules, analyse, score, rank or classify or recommend outcomes.

We take reasonable steps to protect personal information used by these programs and comply with our privacy, confidentiality and information security obligations. Some programs are provided by third parties that may process your personal information outside Australia. See “Disclosure of personal information overseas”.

The table below describes the personal information these programs use and the decisions they help us and our representatives make.

Area	Personal information that may be used	Decisions the programs help make
Financial advice	Personal and financial information, objectives, preferences, health information; answers to questions about risk tolerance.	Advice strategies, asset allocation, product options, portfolio construction and investment recommendations or approvals.
Identity, fraud and anti-money laundering*	Personal and financial information, date of birth, identification documents, citizenship or residency, beneficial ownership, sanctions, occupation, public positions held, associations, and fraud indicators.	Identity verification, fraud flags, risk classification, enhanced due diligence, client acceptance, escalation, and restricting or refusing transactions or services.
Complaints, breaches and remediation	Personal and financial information, advice, product and transaction information, complaint details, loss information, adviser records, correspondence and case information.	Complaint responses, compensation, remediation, reporting obligations.
Representative, authorisation, monitoring and supervision	Personal and financial information, advice records, loan files, audit findings, incidents and breaches, qualifications and training.	Authorisation, recognition of qualifications, audit outcomes, supervision or restrictions to the provision of services or products.
Recruitment and employment	Personal information, qualifications, employment history, skills, conduct, performance and employment records.	Candidate shortlisting or rejection, performance ranking, promotion, remuneration.
Payments	Employee, representative, contractor or supplier details; remuneration, banking, expenses, payment and revenue information.	Payment entitlements, approvals or withholding.

None of these decisions is made solely by a computer program. A person reviews the program's output and makes or confirms the final decision.

If you would like more information about how a program was used in a decision about you, or would like the decision reviewed, contact your financial adviser or our Privacy Officer. Contact details are provided under "Contacting us about privacy".

Complaints about privacy

If you have any privacy related questions or would like further information on our privacy and information handling practices or are concerned about how your personal information has been collected, used or disclosed and you wish to make a complaint, please contact us.

Mail PO Box 392, North Sydney NSW 2059
Phone 02 8247 9900
Email admin@sherlockwealth.com
Website www.sherlockwealth.com

We will acknowledge receipt of a complaint within 1 business day, however, where this is not possible, acknowledgement will be made as soon as practicable. We will then investigate the complaint and respond to you within 30 days. Some complex matters may require an extension to thoroughly investigate the complaint and bring it to resolution. If additional time is required, we will advise you in writing.

If you are not fully satisfied with our response, you can contact an external body. In cases of privacy related complaints, this is generally the Office of the Australian Information Commissioner (OAIC).

The contact details for OAIC are:

Mail	GPO box 5218 Sydney NSW 2001
Phone	1300 363 992
Email	enquiries@oaic.gov.au
Online	www.oaic.gov.au

You may also direct privacy complaints related to financial advice to the Australian Financial Complaints Authority (AFCA). The contact details for AFCA are:

Mail	GPO Box 3, Melbourne, VIC 3001
Phone	1800 931 678 (free call)
Email	info@afca.org.au
Online	www.afca.org.au

About this Policy

We may amend or update our Privacy Policy as required by law or as our business processes, technology or legal and regulatory changes. We will post the updated policy on our website – www.sherlockwealth.com. We encourage you to check our website from time to time to view our current policy or contact us for a printed copy.