Privacy Policy

This Privacy Policy explains how Australian Adviser Group Pty Ltd ("AAG") (we, us or our), collects, holds, uses and discloses personal information. It also applies to AAG's Representatives (including Australian Financial Advisers ("AFA")). We maintain privacy governance arrangements appropriate to the nature and sensitivity of the personal information we handle. Our Privacy Officer coordinates privacy enquiries, access and correction requests, complaints, privacy incidents and eligible data-breach responses.

Protecting your personal information is fundamental to the professional services we provide. As a financial planning business, we collect, use, hold and disclose personal information so that we can understand your circumstances, provide financial products and services, meet our legal obligations and maintain the integrity of our business operations.

We are committed to managing personal information in accordance with the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs) and applicable regulatory requirements. We maintain policies, procedures and systems designed to ensure personal information is handled lawfully, securely and transparently.

Further information about privacy rights and obligations can be obtained from the Office of the Australian Information Commissioner (OAIC) at www.oaic.gov.au

This Policy explains:

- the kinds of personal information we collect and hold;
- how we collect and hold it;
- why we collect, use and disclose it;
- how you may access or correct it;
- how to make a privacy complaint; and
- whether we are likely to disclose it overseas and, where practicable, the countries involved.

1. Privacy Governance

We maintain a Privacy Governance Framework designed to ensure compliance with privacy legislation and regulatory expectations. Our senior management appoints the Privacy Officer. The Privacy Officer oversees privacy compliance and coordinates access and correction requests, complaints, incidents and regulatory liaison. A nominated delegate performs this role during an absence.

Significant privacy incidents are escalated in accordance with our incident-response and governance procedures.

The Privacy Officer is responsible for:

- oversight of privacy compliance;
- management of privacy complaints;
- responding to access and correction requests;
- management of privacy incidents and data breaches;
- liaison with regulators where required; and

- periodic review of this Privacy Policy.

Our nominated Privacy Officer is:

Ava Aram
Telephone: 07 3703 2110
Email: admin@aagnet.com.au
Address: Level 4, 240 Queen Street, Brisbane QLD 4000
Post: PO Box 328, Paddington, QLD, 4064

2. Privacy collection notices

When we collect personal information, we may provide you with additional privacy notices explaining the circumstances of the collection, the purposes for which the information is being collected and other information required by applicable privacy laws. These notices supplement this Privacy Policy.

3. Types of personal information that we collect, use and hold

We may collect and hold a range of personal information about you to provide you with our services. Depending on the services sought, this may include:

- personal identification information and documents;
- date of birth;
- contact information;
- financial circumstances;
- income, expenditure, assets and liabilities;
- superannuation information;
- insurance information;
- taxation information;
- trust and company information;
- beneficiary information;
- family commitments;
- personal information about family and dependents;
- social security eligibility;
- risk profile and investment preferences;
- retirement objectives;
- adviser file notes, communications, recordings and transcripts;
- financial goals and objectives;
- digital identifiers;
- complaint information;
- employment information; and
- health information where relevant to insurance or advice services.

We only collect sensitive information where reasonably necessary and permitted by law. We may collect government-related identifiers, such as tax file numbers or information contained in government-issued

identification documents, where collection is authorised or required by law or is reasonably necessary for a lawful verification process. We do not adopt government-related identifiers as our own identifiers and only use or disclose them where permitted by law.

4. Why we collect your personal information

As a financial service business with an Australian Financial Services Licence we are subject to certain legislative and regulatory requirements, which necessitate us obtaining and holding detailed information, which personally identifies a client and/or contains information or an opinion about a client ("personal information"). We may use and disclose the information we collect about you for the following purposes:

- establishing and verifying your identity;
- checking whether you are eligible for our services;
- assessing your circumstances;
- providing you with our services;
- managing and administering our services;
- providing information we believe may be relevant or of interest to you;
- notifying you of products and services;
- marketing;
- data analytics and statistical analysis;
- maintaining advice and compliance records;
- managing complaints and claims;
- preventing fraud and cyber incidents;
- to notify you of other products, services, special offers or events;
- where you otherwise expressly consent to the use or disclosure;
- complying with legislative and regulatory requirements in any jurisdiction; and
- to assist AAG in the running of our business.

We may use and disclose your personal information for any of these purposes. We may also use and disclose your personal information for secondary purposes which are related to the primary purposes set out above, or in other circumstances authorised by the Privacy Act.

We may be required or authorised to collect particular information under laws that apply to our services, including the Corporations Act 2001 (Cth), the Australian Securities and Investments Commission Act 2001 (Cth), the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth), taxation laws and other applicable legislation. The information required depends on the service provided and the legal obligation concerned.

Sensitive information will be used and disclosed only for the purpose for which it was provided (or a directly related secondary purpose), unless you agree otherwise, or an exemption in the Privacy Act applies.

We retain records for periods required under applicable financial services, taxation, anti-money laundering and other legal obligations. Where personal information is no longer required and we are not required to retain it by law, we take reasonable steps to securely destroy or de-identify that information.

Failure to provide the personal information may affect the adequacy or appropriateness of advice that we can provide. If you do not wish to provide us with the personal information referred to above, we may elect to terminate our services and/or engagement with you if we believe we are unable to provide the complete service.

You may deal with us anonymously or using a pseudonym where this is lawful and practicable, such as when making a general enquiry. This will generally not be practicable where we provide personal financial advice, implement a financial product, verify identity or maintain records required by law.

5. Electronic Identity Verification and Regulatory Requirements

Where AML/CTF laws apply to a service we provide, we may collect and verify information about identity, beneficial ownership, control, customer risk and, where required, source of funds or source of wealth. The information and checks required depend on the designated service, customer type and risks identified. We may use approved electronic verification and screening providers and disclose relevant information to them for these purposes.

This may include the use of electronic verification and compliance screening services to perform customer due diligence, including identity verification, sanctions screening, politically exposed person (PEP) screening and other risk-based checks required by law. Information collected for AML/CTF purposes may be disclosed to service providers engaged to perform these verification and screening activities on our behalf.

We may use electronic identity verification services to verify information you provide and to assist us to meet our legal and regulatory obligations. This may involve providing your name, date of birth, address and identification document details to an approved identity verification provider and matching that information against relevant records or data sources.

Where consent is required for a particular electronic verification process, we will provide the relevant notice and obtain the consent required before undertaking that verification. Where verification is otherwise authorised or required by law, we may undertake those checks in accordance with the applicable legal requirements.

6. How we collect your personal information

We generally collect personal information directly from you. For example, personal information will be collected through our application processes, meetings, phone calls, emails, forms and other interactions with you in the course of providing you with our services.

We may also collect your information from your representatives or professional advisers and electronically (e.g. online forms, email, website interactions).

We will not collect sensitive information about you without your consent unless an exemption in the APPs applies. These exceptions include if the collection is required or authorised by law, or necessary to take appropriate action in relation to suspected unlawful activity or serious misconduct.

If the personal information we request is not provided by you, we may not be able to provide you with the benefit of our services or meet your needs appropriately.

We don't usually collect unsolicited personal information. Where we receive unsolicited personal information that is not relevant, we will destroy or de-identify that personal information as soon as practicable.

7. Disclosure of your personal information

In order to provide you with services, we may need to disclose your personal information to third parties. The organisations that we are likely to disclose information about you to include:

(a) to any of AAG's related companies/entities;
(b) our agents, contractors and external service providers;
(c) technology and cyber security providers;
(d) custodians and platform operators;
(e) product issuers;
(f) professional advisers;
(g) insurers;
(h) regulators;
(i) professional industry bodies (such as Chartered Accountants Australia and New Zealand (CA ANZ));
(j) to our professional advisers, auditors and insurers;
(k) your representatives;
(l) the Australian Financial Complaints Authority or Office of the Australian Information Commissioner;
(m) organisations involved in a transfer or sale of our assets or business;
(n) anyone to whom the disclosure is required or permitted under the Privacy Act, other Australian Law, Regulation or Court/Tribunal Order; and
(o) anyone else where you have provided your consent.

Before disclosing information to service providers who handle personal information on our behalf, we seek to ensure appropriate contractual, confidentiality, privacy and information security protections are in place.

8. Recording of communications

AAG may record or transcribe meetings and telephone calls where lawful and after giving appropriate notice. We use recordings and transcripts to prepare accurate file notes and advice records, support the services we provide and meet legal, regulatory and compliance obligations. Access is limited to authorised personnel and approved providers, and the records are retained in accordance with our retention requirements. If you object to recording, tell us before recording begins so we can consider an appropriate alternative method of maintaining the required record.

Recordings and transcripts will be treated as personal information and handled in accordance with this Policy and applicable privacy laws, including through appropriate security, access and retention controls.

9. Overseas Providers

We utilise reputable technology, cloud-based and professional service providers (such as Microsoft and Xero) to support the delivery of our services and the operation of our business. While personal information is generally stored in Australia, some information may be processed, accessed, supported or backed up in overseas jurisdictions as part of the services provided by these organisations. Overseas recipients may include cloud hosting providers, software vendors, information technology support providers, cybersecurity providers and other professional service providers engaged by us.

Where personal information is handled outside Australia, we take reasonable steps to ensure appropriate privacy, confidentiality and information security safeguards are in place. These measures may include contractual privacy

obligations, due diligence assessments, security reviews and ongoing oversight of our service providers. We seek to engage providers that maintain robust privacy, data protection and information security standards appropriate to the nature and sensitivity of the personal information they handle.
The countries in which overseas recipients are located will depend on the service providers we engage and the locations from which they deliver their services or maintain their technology infrastructure and support operations.

We may disclose personal information to overseas recipients, including service providers that support our technology, cloud hosting, communications, cybersecurity, identity verification and other business operations. Where practicable, those recipients may be located in Australia, Singapore, the United States. The countries involved may change where our service providers change their processing or support locations.

10. Keeping your personal information accurate and up-to-date

We are committed to ensuring that the personal information we collect, use and disclose is relevant, accurate, complete and up-to-date.
We encourage you to contact us to update any personal information we hold about you. If we correct information that has previously been disclosed to another entity, we will notify the other entity within a reasonable period of the correction. Where we are satisfied information is inaccurate, we will take reasonable steps to correct the information within 30 days, unless you agree otherwise. We do not charge you for correcting the information.

11. How we hold and protect your personal information

We recognise the importance of securing the personal information of our clients, we will primarily hold information about you electronically on secure servers located in Australia.

We take reasonable administrative, technical and physical steps to protect personal information from misuse, interference, loss and unauthorised access, modification or disclosure. Depending on the system and risk, safeguards may include:

- multifactor authentication,
- encryption,
- access restrictions,
- monitoring and logging,
- secure backup and recovery,
- staff training,
- vendor assurance,
- secure disposal and incident-response arrangements.

No method of storage or transmission is completely secure.

Security controls are periodically reviewed having regard to the nature, volume and sensitivity of information held by our business.

12. Direct marketing

We may only use personal information we collect from you for the purposes of direct marketing without your consent if:

- the personal information does not include sensitive information;
- you would reasonably expect us to use or disclose the information for the purpose of direct marketing;

- we provide a simple way of opting out of direct marketing; and
- you have not requested to opt out of receiving direct marketing from us.

If we collect personal information about you from a third party, we will only use that information for the purposes of direct marketing if you have consented (or it is impracticable to obtain your consent), and we will provide a simple means by which you can easily request not to receive direct marketing communications from us. We will draw your attention to the fact you may make such a request in our direct marketing communications.

You have the right to request us not to use or disclose your personal information for the purposes of direct marketing, or for the purposes of facilitating direct marketing by other organisations. We must give effect to the request within a reasonable period of time. You may also request that we provide you with the source of information. If such a request is made, we must notify you of the source of the information free of charge within a reasonable period of time. You can opt out of marketing at any time by contacting us.

13. Use of our Website, Social Media and Privacy

The below provides important information about how we use cookies and how we may collect information when you visit our website (https://australianadvisergroup.au/)

AAG use social media to share content and knowledge. You acknowledge any personal information you share over social media is available to other users over which AAG have no control.

13.1 Links to Third-Party Websites

Our website may contain links to third-party websites that are not operated or controlled by AAG. These third-party sites have their own privacy policies and practices, and we encourage you to review them before providing any personal information.

We are not responsible for the content, privacy practices, or the accuracy of information on third-party websites linked to or from our site. These links are provided for your convenience, and their inclusion does not imply that we endorse or are affiliated with the third-party websites.

13.2 What Are Cookies?

Cookies are small text files that are placed on your device (such as your computer or mobile phone) when you visit our website. They help us improve your experience on the website by allowing us to remember your preferences, provide personalised content, and analyse the way visitors use the website. Our website may use necessary cookies and, where enabled, analytics or preference cookies.

We use cookies and similar technologies as described below. Where consent is required for a particular cookie or technology, we will seek that consent through our website or cookie-management tools.

- Necessary Cookies: These cookies are essential for the operation of the website and cannot be disabled in our systems. They are typically only set in response to actions you take, such as logging in or filling out forms.
- Performance Cookies: These cookies collect information about how you use our website, such as which pages you visit most often. They help us improve the functionality of the website by providing insights into user behaviour.
- Functionality Cookies: These cookies enable the website to remember choices you make, such as your preferred language or region, to provide a more personalised experience.

13.3 How We Use Cookies:

We use cookies to:

- Improve your user experience on our website.
- Provide analytics about how our website is used.
- Remember your preferences and settings.

13.4 Privacy and Data Security

We take your privacy seriously. The information collected through cookies is used in accordance with our Privacy Policy. We will not use cookies to collect personally identifiable information without your consent.

14. Your Consent

By using our website, you consent to the use of cookies as outlined in this policy. If you do not agree with our use of cookies, you can manage your cookie preferences by adjusting your browser settings. You can choose to block or delete cookies; however, please note that this may affect the functionality of certain parts of the website.

AAG uses electronic signing platforms. We do not verify the signature upon receipt of signed documents and it is the responsibility of the individual to satisfy themselves of the security controls and integrity over the electronic signature process utilised by them. You remain responsible for reviewing all documentation prior to execution. By engaging with AAG, you consent to the use of electronic signing platforms.

15. Use of Artificial Intelligence (AI) technology

We utilise artificial intelligence (AI) and automation technologies within our business, including Microsoft Copilot and Microsoft Teams to assist with administrative, operational and record-keeping activities.

Examples may include:

- meeting transcription;
- note preparation;
- document summarisation;
- workflow automation;
- research assistance; and
- operational efficiency activities.

AI technologies are used as support tools only. We conduct risk assessments before deploying AI systems that process personal information. AI-generated outputs are reviewed by appropriately authorised personnel before being relied upon for client servicing, compliance or operational purposes.

We do not permit AI systems to independently provide personal financial advice, make decisions about your financial advice or your personal circumstances or make decisions regarding the suitability of advice provided to clients. We do not currently use a computer program to make decisions that could reasonably be expected to significantly affect an individual's rights or interests.

Where personal information is processed through AI-enabled systems, we seek to ensure appropriate privacy, security and governance controls are in place. We periodically review AI-enabled technologies as part of our risk management, privacy and cyber security framework.

You may ask us not to use optional client-facing AI functions, such as meeting transcription or automated meeting summaries, by contacting admin@aagnet.com.au. We will explain any practical effect on the service and use an appropriate alternative where reasonably available. This choice does not apply to essential security, fraud

prevention, spam filtering, legal record keeping or other processing that is necessary to provide the service or meet our obligations.

16. Cyber Security and Operational Resilience

As a financial services business, we recognise the importance of protecting client information and maintaining operational resilience. We maintain cyber security and operational risk management controls that are designed to support the confidentiality, integrity and availability of the information we hold.

Our cyber security framework is periodically reviewed having regard to evolving threats, regulatory expectations and business operations.

17. Gaining access to your personal information

You can gain access to your personal information (subject to some exceptions allowed by law) by contacting the Privacy Officer. We will need to verify your identity first.

We will provide you access within 30 days if it is reasonable and practicable to do so, but in some circumstances, it may take longer (for example, if we need to contact other entities to properly investigate your request or retrieve information from archived systems).

We may refuse to provide you with access in certain circumstances. If access is refused, we will give you a notice explaining the reasons for our decision and your options to make a complaint.

We do not usually charge you for access to your personal information. However, if the request is complex, we may charge you the marginal cost of providing the access, such as staff costs of locating and collating information or copying costs. If charges are applicable in providing access to you, we will disclose these charges to you prior to providing you with the information.

18. Data Breaches

We maintain procedures to contain and assess suspected privacy incidents and data breaches, take remedial action where possible and escalate matters appropriately. Where we have reasonable grounds to believe an eligible data breach has occurred, we will notify affected individuals and the Office of the Australian Information Commissioner in accordance with the Notifiable Data Breaches scheme. We review incidents to identify and implement appropriate control improvements.

19. Resolving your privacy concerns

If you have a privacy concern or complaint, please contact our Privacy Officer using the contact details provided below. We will acknowledge your complaint promptly and aim to provide a written response within 30 days. Where appropriate, we may:

- investigate the matter;
- seek further information;
- attempt informal resolution;
- implement corrective actions; and
- provide reasons for our decision.

If you remain dissatisfied, you may contact the Office of the Australian Information Commissioner or the Australian Financial Complaints Authority.

Online: www.afca.org.au
Email: info@afca.org.au
Phone: 1800 931 678
Mail: Australian Financial Complaints Authority GPO Box 3 Melbourne VIC 3001

You may also contact the Office of the Australian Information Commissioner by:
Online: www.oaic.gov.au
Email: enquiries@oaic.gov.au
Phone: 1300 363 992
Mail: Director of Complaints, Office of the Australian Information Commissioner GPO Box 5218, Sydney NSW 2001

Please see our Complaints Policy available on our website at https://australianadvisergroup.au/ for full details of how we deal with complaints.

20. Contact Us:

Telephone: 07 3703 2110
Email: admin@aagnet.com.au
Address: Level 4, 240 Queen Street, Brisbane QLD 4000
Post: PO Box 328, Paddington, QLD, 4064

This Privacy Policy is available free of charge and may be provided in an alternative format upon request.

Last Updated: 16 November 2026

21. Policy Review

This Privacy Policy will be reviewed at least annually and may also be reviewed more frequently following any material legislative or regulatory change, significant privacy incident or data breach, implementation of significant new technology, introduction of material artificial intelligence (AI) capabilities, or where there is a material change to the nature, scale or operations of the business.

The purpose of these reviews is to ensure that this Privacy Policy remains accurate, current and consistent with applicable legal obligations, regulatory expectations and our privacy governance framework.

DOCUMENT HISTORY

Version	Date	Reviewed by
1.0	**November 2026**	**3Lines Consulting**
Description:	**New Policy – Previous version archived.**	