ALLIED FINANCIAL SOLUTIONS PTY LTD

Privacy Policy

Privacy practices for clients, prospective clients and business contacts

Allied Financial Solutions Pty Ltd
AFSL 230172
ABN 37 092 222 412

Unit 1B, 4 Rocklea Drive
Port Melbourne, VIC 3207
Ph: 03 7019 3111
admin@alliedfingroup.com

Document control	Details
Version	3.0
Effective date	16 September 2026
Reviewed by	Compliance Manager
Approved by	Director
Next review date	16 September 2027
Supersedes	Privacy Policy v3.0

Status Formatting and document-control standardisation; no substantive policy changes.

Contents

1. Who we are and how to contact us
2. What this policy covers
3. The personal information we collect
4. How we collect personal information
5. Why we collect, use and disclose personal information
6. Direct marketing
7. Disclosing personal information
8. Overseas disclosures
9. Our website, cookies and third-party links
10. Data security
11. Retention and destruction
12. Data breaches and notification
13. Access and correction
14. Children's information
15. Your choices and rights
16. Changes to this policy
17. How to make a privacy complaint
18. Additional notices for AML/CTF compliance
19. Definitions
Quick summary (not part of the policy)
Version history

1. Who we are and how to contact us

Contact	Details
Responsible entity	Allied Financial Solutions Pty Ltd
Privacy contact	Kenneth Henning, Director
Email	admin@alliedfingroup.com
Phone	+61 3 7019 3111
Address	1B, 4 Rocklea Drive Port Melbourne VIC 3207

We are committed to protecting your privacy. This policy explains how we manage personal information in line with the Australian Privacy Principles (APPs) under the Privacy Act 1988 (Cth), and (for health information handled in Victoria) the Health Records Act 2001 (Vic) and its Health Privacy Principles (HPPs). If we are a reporting entity under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) (AML/CTF Act), the small business exemption to the Privacy Act does not apply to us.

2. What this policy covers

This policy applies to personal information we collect and handle in the course of providing financial planning and related services to clients and prospective clients, including via our website, client portal, email, phone and in person. It also applies to job applicants, contractors and suppliers.

3. The personal information we collect

The types of information we may collect include:

- Identification & contact: name, date of birth, residential and postal addresses, email, phone, occupation, government identifiers (e.g., driver licence or passport number) where required by law (e.g., KYC/AML).
- Client profile & advice information: goals and objectives, risk tolerance, time horizon, financial situation, investment preferences, superannuation and insurance details, income, assets and liabilities, expenses, tax residency and TFN (only where permitted/required by law), beneficiary details.
- Sensitive information (only with consent or as permitted by law): health and medical information relevant to insurance or advice suitability; membership of professional or trade associations if relevant.
- Transaction & interaction data: records of communications, meeting notes, instructions, file notes, documents provided to or generated by us, engagement letters, authorities to proceed, advice records (e.g., SoAs/ROAs).
- Website/portal data: IP address, device/browser type, pages visited, session duration, cookies and analytics; portal login and usage metadata.
- Employment & supplier data: resumes/CVs, referees, qualifications, background checks (where permitted), ABNs, bank details for payments.

We avoid collecting government-related identifiers (e.g., Medicare numbers, TFNs) unless required or authorised by law and will not use them as our own identifiers.

4. How we collect personal information

We collect information:

- Directly from you: when you enquire, meet with us, complete fact finds, provide documentation, use our website or client portal, respond to surveys, or subscribe to updates.
- From third parties with your authority or where permitted by law: superannuation funds, insurers, product issuers, investment platforms, administrators, accountants, mortgage brokers, other advisers, credit bureaus (if relevant), identification verification services, and public sources.
- Automated means: via cookies and similar technologies on our website and client portal. You can usually disable cookies in your browser, but this may affect site functionality.

Where it is lawful and practicable we will give you the option of not identifying yourself or using a pseudonym, but this may limit our ability to provide services that require identity verification.

5. Why we collect, use and disclose personal information

We handle personal information to:

- provide, administer and improve our financial planning services (including advice preparation, implementation and ongoing reviews);
- verify your identity and comply with AML/CTF, taxation and other legal obligations;
- conduct compliance, quality assurance and audits, and manage risk, training and record-keeping;
- communicate with you about your engagement, requested services, and relevant regulatory or product updates;
- manage our business operations, IT systems and security;
- send marketing communications (you can opt out at any time);
- handle queries, feedback and complaints.

We only collect sensitive information (such as health information) with your consent or where required/authorised by law and only for purposes directly related to our services (e.g., insurance underwriting or advice suitability).

6. Direct marketing

We may use your contact details to send you information about our services or events that may be of interest. You can opt out at any time by using the unsubscribe link in emails or by contacting us. We comply with the Spam Act 2003 (Cth) for electronic marketing.

7. Disclosing personal information

We may disclose personal information to:

- product issuers, superannuation funds, insurers, investment platforms and administrators to implement your instructions;
- third-party service providers who support our operations (e.g., paraplanners, IT/cloud providers, client portal providers, document storage/archiving, identity verification, analytics, auditors and professional advisers);
- regulators and authorities (e.g., AUSTRAC, ASIC, ATO, OAIC) where required or authorised by law;
- your nominated representatives and other professional advisers (e.g., accountants, solicitors) with your consent;
- our related entities (if any) for the purposes described in this policy.

Where we engage third parties, we require them to handle personal information in accordance with applicable privacy laws and our instructions.

8. Overseas disclosures

Allied Financial Solutions Pty Ltd primarily stores personal information using systems and service providers that maintain data within Australia.

However, some of our technology providers, software vendors and cloud-based service providers may store, process or provide technical support for personal information using infrastructure or personnel located outside Australia. This may include providers of financial planning software, investment platforms, cloud storage, email services, identity verification services and other business support systems.

Before disclosing personal information overseas, or engaging a service provider that may access personal information from outside Australia, we will take reasonable steps to ensure the recipient handles the information in a manner consistent with the Australian Privacy Principles. These steps may include contractual obligations, due diligence of service providers and reliance on recognised privacy and security standards.

Where personal information is disclosed overseas, Allied Financial Solutions Pty Ltd may remain accountable for the handling of that information under the Privacy Act 1988 (Cth).

9. Our website, cookies and third-party links

Our website and client portal may use cookies and similar technologies to improve functionality and analytics. You can control cookies through your browser settings. Our site may contain links to third-party websites; we are not responsible for their privacy practices. We recommend you review their privacy policies.

10. Data security

Despite these measures, no method of transmission or storage is completely secure. If a suspected or actual data breach occurs, Allied Financial Solutions Pty Ltd will promptly investigate the incident, take appropriate steps to contain and remediate the breach, assess whether it is an eligible data breach under the Notifiable Data Breaches (NDB) scheme, and respond in accordance with the procedures set out in this Policy.

11. Retention and destruction

We retain personal information for as long as needed to provide services and to comply with legal, regulatory and professional obligations (for example, financial services and taxation record-keeping requirements). Health information records in Victoria are generally retained for at least seven (7) years from the last entry (or longer where required). When no longer required, we will take reasonable steps to destroy or de-identify information securely.

12. Data breaches and notification

If Allied Financial Solutions Pty Ltd becomes aware of, or suspects, a data breach involving personal information, the Compliance Officer will promptly investigate the incident and take reasonable steps to contain and mitigate any ongoing risk.

The Compliance Officer will assess whether the incident is likely to constitute an eligible data breach under the Privacy Act 1988 (Cth) and the Notifiable Data Breaches (NDB) Scheme.

Where an eligible data breach is identified, Allied Financial Solutions Pty Ltd will:

- take reasonable steps to contain and remediate the breach;
- assess the nature and extent of the information affected;
- notify affected individuals as soon as practicable where required by law;
- notify the Office of the Australian Information Commissioner (OAIC) in accordance with legislative requirements; and
- maintain appropriate records of the incident, actions taken and any remedial measures implemented.

Following any significant data breach, Allied will review the circumstances of the incident and implement any appropriate improvements to its privacy, information security or operational procedures.

13. Access and correction

You can request access to the personal information we hold about you and ask us to correct it if it is inaccurate, out-of-date, incomplete, irrelevant or misleading. We will respond within a reasonable period (usually within 30 days). We may need to verify your identity and, in rare cases, may refuse access where permitted by law (we will tell you why and how you can complain). We do not charge to make a request, and any access fees (if applicable) will be limited to reasonable administration costs.

14. Children's information

Our services are generally directed to adults, but we may collect information about children (e.g., as beneficiaries) with the consent of a parent or legal guardian and only where necessary.

15. Your choices and rights

- You may opt out of marketing at any time.
- You may deal with us anonymously or under a pseudonym where lawful and practicable.
- You may withdraw consent to our handling of sensitive information (where consent is the lawful basis), noting this may affect our ability to provide certain services.

16. Changes to this policy

We may update this policy from time to time. The latest version will be published on our website. Material changes will be communicated where appropriate.

17. How to make a privacy complaint

If you have a question or complaint about how we handle your personal information, please contact us using the details above. We will acknowledge your complaint promptly and aim to respond in writing within 30 days. If you are not satisfied with our response, you may contact:

Office of the Australian Information Commissioner (OAIC)
GPO Box 5288, Sydney NSW 2001
Phone: 1300 363 992
Online: search "OAIC lodge a privacy complaint"

For health information in Victoria:
Health Complaints Commissioner (HCC)
Level 26, 570 Bourke Street, Melbourne VIC 3000
Phone: 1300 582 113
Online: search "HCC make a complaint"

18. Additional notices for AML/CTF compliance

If we are required to perform customer due diligence under the AML/CTF Act, we may:

- collect and verify identification information (e.g., via accredited electronic verification providers);
- disclose information to and obtain information from AUSTRAC and other reporting bodies where required by law; and
- retain records for the periods required by the AML/CTF Act and Rules.

19. Definitions

Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable.

Sensitive information includes health information and information about an individual's racial or ethnic origin, political opinions, religious beliefs, sexual orientation, and membership of professional or trade associations.

Health information has the meaning given in the Health Records Act 2001 (Vic).

Quick summary (not part of the policy)

- We collect the minimum personal information we need to provide advice and meet legal obligations.
- We won't sell your personal information.
- You can access and correct your information and opt out of marketing.
- If a serious data breach occurs, we'll tell you and the OAIC.

Version history

Version	Date	Description	Approved by
3.0	16 September 2026	Formatting and document-control standardisation; no substantive policy changes.	Director