Privacy Policy

Apex Financial Advice (ABN 20 628 881 096),

Authorised Representative (1319167) of Apex FSG PTY LTD, AFSL 539244

Version [2.0] | Effective 15/11/2026 |

1. About this policy

Apex Financial Advice (**we**, **us**, **our**) is a financial advice practice based in Queensland, Australia. We are committed to protecting the privacy of the people we deal with, and we handle personal information in accordance with the *Privacy Act 1988* (Cth) (**Privacy Act**) and the Australian Privacy Principles (**APPs**).

This policy explains what personal information we collect, why we collect it, how we use and disclose it, how we keep it secure, and how you can access or correct it or make a complaint. It applies to clients, prospective clients, their family members and associated persons, referrers, job applicants, and visitors to our website.

We may update this policy from time to time. The current version is always available on our website or by contacting us.

2. What is personal information?

Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether or not the information is true and whether or not it is recorded in a material form.

Sensitive information is a subset of personal information and includes information about health, racial or ethnic origin, political opinions, religious beliefs, memberships of professional or trade associations or unions, sexual orientation, criminal record, and biometric information. Sensitive information is afforded a higher level of protection under the Privacy Act.

3. The personal information we collect

The information we collect depends on the services we provide to you. It may include:

Identity and contact details

- Full name, date of birth, gender, residential and postal address, phone numbers and email addresses
- Photo identification and other documents used to verify your identity (for example, drivers license, passport, Medicare card, birth certificate)
- Marital or relationship status, details of dependants and family members

Financial and personal circumstances

- Employment details, income, expenses, assets, liabilities and cash flow
- Superannuation, pension and insurance details, including policy and member numbers

- Investment holdings, bank and loan account details, and credit information you provide
- Taxation information, including your Tax File Number (TFN) where you choose to provide it
- Your goals, objectives, needs, risk tolerance, financial knowledge and experience
- Estate planning information, such as wills, powers of attorney and beneficiary nominations

Sensitive information (only where necessary)

- Health and lifestyle information, including medical history, smoking status and family medical history, where this is relevant to personal insurance advice or to your capacity to work and retire
- Information about disability, financial hardship or vulnerability, so that we can provide appropriate advice and support
- Citizenship and residency status, where required for identification, tax or legal purposes

Other information

- Records of our communications with you, including file notes, emails, letters, and recordings of phone or video meetings
- For job applicants: résumé, work history, qualifications, referee details and police or background check results

4. How we collect personal information

We collect personal information in the following ways:

- **Directly from you**, through meetings, phone calls, emails, fact-finds and questionnaires, application forms, our website and client portal, and documents you give us
- **From third parties with your consent or as authorised by law**, such as your accountant, lawyer, mortgage broker, employer, superannuation funds, insurers, platform and product providers, the Australian Taxation Office (**ATO**) or Services Australia (for example through online portals where you have authorised us), and credit reporting bodies
- **From publicly available sources**, such as public registers, social media and online directories
- **From referrers**, such as other professionals or existing clients who refer you to us
- **From identity verification services** used to meet our obligations under anti-money laundering laws

We collect personal information about you only from you where it is reasonable and practicable to do so. If we receive personal information we did not ask for (unsolicited information) and we determine we could not have collected it, we will destroy or de-identify it as soon as practicable, where lawful and reasonable to do so.

If you give us personal information about another person (for example, a spouse, child, or beneficiary), you should make sure that person knows you have done so and is aware of this policy.

5. Why we collect, hold, use and disclose personal information

We collect personal information that is reasonably necessary for our functions and activities. Our main purposes are to:

- verify your identity and meet our KYC and AML/CTF obligations
- understand your personal and financial circumstances, objectives and needs
- provide you with personal financial advice and related services, including preparing a Statement of Advice or Record of Advice, implementing recommendations, and providing ongoing advice and review services
- arrange, apply for, manage and administer financial products and services on your behalf, such as superannuation, investments, insurance, loans and platforms
- meet our legal and regulatory obligations (see section 6)
- manage our relationship with you, including billing, fee disclosure and consent processes, handling enquiries, and resolving complaints
- carry out internal functions such as record keeping, quality assurance, compliance monitoring and audits, training, business planning and risk management
- tell you about our services, events, and information that may interest you (see section 9)
- protect against fraud, misconduct and unlawful activity

We will generally use or disclose your personal information only for the primary purpose for which it was collected, or for a related purpose you would reasonably expect (or, for sensitive information, a directly related purpose). We will otherwise obtain your consent or rely on another exception permitted under the Privacy Act, such as where use or disclosure is required or authorised by law.

If you do not provide the information we ask for, we may not be able to provide you with our services. In particular, under the *Corporations Act 2001* (Cth) we must make reasonable enquiries about your relevant circumstances so that our advice is appropriate to you. Incomplete or inaccurate information may mean our advice is not suitable for you.

6. Laws that require or authorise us to collect information

We are required or authorised by law to collect certain personal information, including under:

- the *Corporations Act 2001* (Cth) and associated regulations and ASIC requirements, including the best interests duty, advice and record-keeping obligations, and the Financial Advisers Register
- the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth), which requires us to verify your identity and report certain matters to AUSTRAC
- the *Insurance Contracts Act 1984* (Cth), which requires disclosure of relevant information to insurers
- the *Superannuation Industry (Supervision) Act 1993* (Cth) and related legislation
- the *Privacy Act 1988* (Cth)

7. Who we may disclose your personal information to

We may disclose your personal information, where necessary for the purposes described above, to:

- **Our licensee** (Apex FSG PTY LTD), who authorises us to provide financial services and is responsible for monitoring and supervising our compliance
- **Product issuers and service providers**, including superannuation funds, platforms, fund managers, insurers, banks, lenders, and their administrators and underwriters

- **Other professional advisers** you have authorised or asked us to work with, such as accountants, solicitors, mortgage brokers, and other financial planners
- **Paraplanning, compliance, audit and administration providers**, including contractors and outsourced service providers who assist us in preparing advice or running our business
- **Technology and data service providers**, including providers of client relationship management (CRM), financial planning software, document storage, email, cloud hosting, e-signature, communications and website services, and cyber security
- **Identity verification providers**
- **Government bodies and regulators** when required, including ASIC, AUSTRAC, the ATO, the Office of the Australian Information Commissioner (**OAIC**), and the Australian Financial Complaints Authority (**AFCA**)
- **Medical practitioners and health service providers**, where you have consented and it is necessary for insurance advice or claims
- **Our professional advisers**, such as lawyers, accountants, auditors and insurers (including professional indemnity insurers)
- **Other persons authorised by you**, such as a person holding your power of attorney, an executor, or a person you have nominated to deal with us on your behalf
- **Prospective purchasers or successors of our business**, and their advisers, who are bound by confidentiality, if our business or client register is sold or restructured
- **Any other person where you have given consent, or where disclosure is required or authorised by law or a court or tribunal order**

We take every reasonable step to ensure that third parties we disclose personal information to are bound by privacy and confidentiality obligations. We do not sell personal information.

8. Automated decision-making and artificial intelligence

We may use automated systems, software tools and artificial intelligence (**AI**) technologies to help us provide financial services, meet our regulatory obligations and improve our client service. These technologies may be developed by us or provided by third-party technology providers.

How we use automated systems and AI

Where relevant to our services, these tools may include:

- client onboarding and identity verification systems
- AML/CTF screening and fraud detection tools
- client risk profiling and risk tolerance assessment tools
- product and portfolio research systems
- portfolio construction, asset allocation and rebalancing tools
- financial modelling and strategy projection software
- client relationship management and workflow systems
- document review and drafting tools
- generative AI tools that assist our staff to analyse information and prepare communications
- compliance monitoring and quality assurance systems

Personal information these systems may use

- identity and contact details
- demographic information
- financial information, including assets, liabilities, income and expenses
- investment objectives and risk profile information
- superannuation and insurance information
- information collected during our interactions with you
- any other information you provide to us in connection with our services

Decisions and recommendations supported by automated systems

Automated systems may assist us to:

- assess client onboarding requirements
- conduct identity verification and regulatory screening
- identify potential fraud, financial crime or cybersecurity risks
- prepare financial projections and model outcomes
- generate investment or insurance research
- construct or review proposed portfolios
- produce draft advice materials and client communications
- identify compliance issues or file review exceptions
- determine whether we need more information from you

Human oversight

Except where required by law or regulatory processes, we do not rely solely on automated systems to make personal financial advice decisions for clients. Our advisers, authorised representatives and staff review and assess information generated by automated systems before making recommendations or taking action. Automated tools assist our personnel but do not replace professional judgment.

Use of generative AI

We may use generative AI to assist with research, document preparation, drafting, summarisation and administrative functions. Where we do:

- information may be processed by approved technology providers, some of which may be located overseas (see section 11)
- we apply controls designed to protect confidential and personal information
- outputs are reviewed by appropriately authorised personnel before we rely on them
- AI-generated outputs are not treated as final advice without human review

Your rights

You can contact our Privacy Officer (see section 19) to ask for more information about our use of automated systems, to access or correct personal information used by them, or to raise concerns about decisions or recommendations informed by automated processing. Sections 17 and 18 explain how to access and correct your information and how to make a complaint.

9. Sensitive information

We collect sensitive information only with your consent (or where otherwise permitted by law) and only where it is reasonably necessary for the services we provide, for example health information for personal risk insurance advice. We will use and disclose sensitive information only for the purpose for which it was collected, for a directly related purpose you would reasonably expect, or as otherwise permitted or required by law.

10. Direct marketing

We may use your name and contact details to send you information about our services, newsletters, market updates and events that we think may interest you. We will do this only where permitted by the Privacy Act and the *Spam Act 2001* (Cth), and you can opt out at any time by contacting us. We will act on your request. We will not use your sensitive information for direct marketing without your consent. We do not give personal information to third parties for their own marketing purposes.

11. Overseas disclosure

Some of our service providers (such as paraplanning providers) may access personal information outside Australia. Countries where this may occur include the Philippines.

Before we disclose personal information to an overseas recipient, we will take reasonable steps in the circumstances to ensure the recipient does not breach the APPs in relation to that information, usually by contractual arrangements.

Our data is stored in Australia.

12. Government related identifiers and Tax File Numbers

We do not adopt a government related identifier (such as a Medicare number or drivers license number) as our own identifier for you. We will use or disclose government identifiers only where this is reasonably necessary to verify your identity, to fulfil our obligations to a government agency, or as otherwise required or authorised by law.

Providing your TFN to us is not compulsory, but if you choose to provide it, we will collect, use, and disclose it only as permitted by tax and privacy law, such as for the purpose of lodging applications with superannuation funds and other providers. We handle TFNs in line with the Privacy (Tax File Number) Rule 2015. Declining to quote your TFN is not an offence, but it may result in tax being withheld at higher rates or other consequences, which we will explain to you.

13. Anonymity and pseudonymity

You have the option of not identifying yourself, or of using a pseudonym, when dealing with us, for example when making a general enquiry. However, we cannot provide personal financial advice or arrange financial products unless we can identify you, as we are legally required to verify your identity and understand your circumstances.

14. Our website and digital services

We do not collect personal information from visitors to our website. The only personal information we receive through our website is what you choose to send us in an enquiry, such as your name, contact details and the nature of your question. We use that information only to respond to your enquiry and, if you become a client, to provide our services, and we handle it as set out in this policy. Our website may contain links to third-party websites that have their own privacy policies; we are not responsible for those sites.

Email and internet communications may not always be secure. If you wish to send us sensitive or confidential information, please contact us by phone.

15. Security, storage and retention

We hold personal information in electronic and, in some cases, paper form. We take every reasonable step to protect it from misuse, interference and loss, and from unauthorised access, modification or disclosure, including through:

- restricting access to personal information to staff and contractors who need it for their role
- password protection, multi-factor authentication, encryption and firewalls on our systems
- secure, access-controlled premises and locked storage for paper records
- confidentiality obligations and privacy training for our staff and contractors
- due diligence and contractual protections for service providers who handle information on our behalf
- regular reviews of our security controls and a data breach response plan

We keep personal information for as long as it is needed to provide our services and for as long as the law requires. Under financial services laws, we are generally required to keep client records, including advice documents, for a minimum of seven (7) years. When personal information is no longer needed and we are not legally required to keep it, we take reasonable steps to securely destroy or de-identify it.

16. Data breaches

We comply with the Notifiable Data Breaches scheme under the Privacy Act. If we experience an eligible data breach, meaning unauthorised access to, or disclosure or loss of, personal information that is likely to result in serious harm, we will promptly assess the incident, take steps to contain it, and notify affected individuals and the OAIC as required by law.

17. Accessing and correcting your personal information

You may 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.

To make a request, contact our Privacy Officer using the details in section 19. We may need to verify your identity before releasing or changing information. We will respond within a reasonable period, generally within 30 days, and will give you access in the manner you request if it is reasonable and practicable to do so. We do not usually charge for making a request, but may charge a reasonable fee to cover the cost of retrieving and supplying the information, and will tell you the amount in advance.

We may refuse access or correction in limited circumstances permitted by the Privacy Act, for example where giving access would unreasonably affect another person's privacy, would be unlawful, or relates to legal proceedings. If we refuse, we will give you written reasons and information about how to complain. If we refuse to correct information, you may ask us to attach a statement to your record that the information is inaccurate, out of date, incomplete, irrelevant or misleading.

18. Complaints

If you believe we have breached the APPs or this policy, please contact our Privacy Officer in writing. We will acknowledge your complaint promptly, investigate it, and aim to give you a response within 30 days.

If you are not satisfied with our response, you may refer your complaint to:

Australian Financial Complaints Authority (AFCA) Website: www.afca.org.au | Phone: 1800 931 678 | Email: info@afca.org.au GPO Box 3, Melbourne VIC 3001

Office of the Australian Information Commissioner (OAIC) Website: www.oaic.gov.au | Phone: 1300 363 992 GPO Box 5288, Sydney NSW 2001

19. Contact us

Privacy Officer
Apex Financial Advice
643 Logan Rd, Greenslopes Qld 4120
07 3180 8831
admin@apexfsg.com.au
www.apexfsg.com.au
www.apexfinancialadvice.com.au

20. Changes to this policy

We may amend this policy from time to time to reflect changes in our practices, technology or the law. The updated policy will be published on our website and is available free of charge on request. We encourage you to review it periodically.