Privacy Policy

Sherpa Financial Group Pty Ltd

ACN 606 750 976
Corporate Authorised Representative No. 1236433
of Integrity Financial Planners Pty Ltd
AFSL 225051

Business address: Suite 1.02, 269 Centre Road, Bentleigh VIC 3204. Phone: 03 7047 9598.

Sherpa Financial Group Pty Ltd Privacy Policy

At Sherpa Financial Group Pty Ltd (SFG), we understand that the privacy of your information is important to you and we respect the confidentiality of the information you provide to us. Protecting your information is an important part of maintaining trust between us and our clients. By handling information securely, we build strong business relationships.

This document explains how we manage the personal information we collect, hold, use and disclose about individuals. This Privacy Policy applies to SFG, its employees and representatives. We are bound by the Australian Privacy Principles established under the Privacy Act 1988 (Cth), as amended. A summary of the Australian Privacy Principles is available from the Office of the Australian Information Commissioner (OAIC) at www.oaic.gov.au. We manage and protect personal information in accordance with the Australian Privacy Principles.

As a registered tax (financial) adviser, SFG and its representatives are also subject to the confidentiality obligations in the Code of Professional Conduct under the Tax Agent Services Act 2009, where applicable.

This Privacy Policy is available free of charge on request and through our website at www.sherpafg.com.au. If you need a copy in another form, please contact us and we will take reasonable steps to provide it.

Who are we

Sherpa Financial Group Pty Ltd (SFG) is a privately owned financial planning business and a Corporate Authorised Representative (No. 1236433) of Integrity Financial Planners Pty Ltd under Australian Financial Services Licence No. 225051.

As our namesake, the Himalayan Sherpa, we pride ourselves on guiding our clients and helping them achieve their ultimate goals. Our approach is comprehensive and holistic, with advice tailored to each client's individual circumstances, goals and objectives. We aim to support and guide our clients throughout their financial planning journey.

Integrity Financial Planners Pty Ltd (Integrity) is a privately owned Australian Financial Services Licensee established in 1995 in Melbourne, Victoria. Integrity has no ownership ties to any fund manager or financial institution and provides licensing solutions to authorised financial advice practices, including SFG. Details of Integrity's current authorised representatives and corporate authorised representatives are available at www.iplan.com.au.

This Privacy Policy explains how SFG collects, holds, uses and discloses personal information in conducting its financial planning business. Where Integrity is specifically referred to in this policy, this relates to Integrity's role as SFG's Australian Financial Services Licensee or another function undertaken by Integrity in connection with SFG's authorised activities.

Why we collect and use personal information

As a financial planning organisation, we are subject to legislative and regulatory requirements, including the Corporations Act 2001 and, where applicable, the Anti-Money Laundering and Counter-Terrorism Financing Act 2006. These requirements mean we need to obtain and hold information about you to provide advice, verify identity and keep required records. Personal information is information or an opinion about an identified individual, or an individual who can reasonably be identified.

We collect, hold, use and disclose personal information so we can provide financial products, advice and services relevant to your needs. Subject to the privacy requirements explained in this policy, we may also collect, use and disclose information for related purposes such as:

- complying with legal obligations, including verifying your identity
- assisting with questions and complaints
- arranging services to be provided by third parties
- internal operations, including record keeping, data analytics, auditing and training
- promoting other products and services that may be of interest to you, where permitted by law

We also collect, use, hold and sometimes disclose personal information about financial advisers, employees and other people with whom we do business in order to administer and manage our operations. This information receives the same standard of care as client information.

What personal information we collect

We ask for a range of personal information to assist us in providing relevant advice, products and services. This may include your name, date of birth, contact details, financial information, employment details, residency and citizenship status. We may also collect personal information about family members where it is relevant to the advice being provided. We collect only information reasonably necessary for our functions or activities. If you provide information about another person, please ensure you have authority to do so and let them know about this policy.

We may collect sensitive information about your medical history, health and lifestyle to provide financial advice about life insurance products. We collect sensitive information with your consent unless the law permits or requires collection without it. In most instances, we collect personal information directly from you when you:

- complete a financial product application form
- complete an identification form
- complete data collection documentation
- interact with an online tool, such as a budget planner
- provide documentation to us
- communicate with us in person, by telephone, fax, email, internet or another electronic device

Where it is unreasonable or impracticable to collect information directly from you, we may collect it from other people and organisations, with your consent where required. These sources may include:

- a financial adviser
- a mortgage broker or another credit representative
- professionals acting on your behalf, such as a lawyer or accountant
- health professionals
- fund managers, superannuation funds, life insurance companies and other product issuers, once authorised
- social media and publicly available sources

If we receive personal information we did not request, we assess whether we could lawfully have collected it. If not, we destroy or de-identify it as soon as practicable where lawful and reasonable. We take reasonable steps to notify people about our collection of their information at or before collection, or as soon as practicable afterwards.

It is your choice whether to provide personal information. You may choose not to provide information, including information about your identity. Your adviser will explain the possible consequences and how this may affect the quality of advice. We may decline to provide advice or services if we do not have sufficient information for the requested scope.

In some circumstances, the law requires us to obtain and verify photographic and non-photographic identification documents.

You can deal with us anonymously or use a pseudonym unless the law requires or authorises us to identify you, or it is impracticable to deal with you that way. For example, you may make a general enquiry anonymously, but we will usually need to identify you to provide personal financial advice.

AI meeting notes and administrative tools

We may use artificial intelligence (AI) tools to assist with administrative tasks, including preparing or summarising meeting notes. This may involve processing information discussed during meetings, including personal information and, where relevant, health information. Before using a tool to record or transcribe a meeting, we will seek your agreement. We review AI-generated notes before relying on them.

Accessing and updating personal information

You can request access to personal information we hold about you by contacting your adviser or the Integrity Compliance Manager using the details below. We may need to verify your identity and the authority of anyone acting for you. There is no charge to make a request. We may charge a reasonable, non-excessive fee for providing access, subject to legal limits. Any cost will be discussed and agreed with you in advance.

We may refuse access only where the law allows or requires it. Commercial sensitivity alone is not enough. Under the Australian Privacy Principles, access may be refused where:

- we reasonably believe access would pose a serious threat to the life, health or safety of a person, or to public health or public safety
- access would have an unreasonable impact on another person's privacy
- the request is frivolous or vexatious
- the information relates to existing or anticipated legal proceedings and would not be discoverable in those proceedings
- access would reveal our intentions in negotiations in a way that would prejudice those negotiations
- access would be unlawful
- denying access is required or authorised by Australian law or by a court or tribunal order
- SFG or Integrity has reason to suspect unlawful activity or serious misconduct and access would likely prejudice appropriate action
- access would likely prejudice enforcement-related activities conducted by or for an enforcement body
- access would reveal evaluative information generated in connection with a commercially sensitive decision-making process

If we refuse access, or refuse access in the way requested, we will provide written reasons unless it would be unreasonable to do so and explain how you can complain. We will consider reasonable alternatives, such as providing part of the information or using an agreed intermediary.

We respond to access and correction requests within a reasonable period, generally within 30 calendar days. We provide access in the requested way if reasonable and practicable. If your request is urgent, please state this clearly.

You may ask us to update your personal information. We take reasonable steps to keep information accurate, up to date, complete and relevant, and to correct information that is inaccurate, out of date, incomplete, irrelevant or misleading. There is no charge to request or make a correction. If we refuse a correction, we will provide written reasons unless unreasonable, explain how to complain and, if requested, take reasonable steps to attach a statement of your concern to the information. If requested, we will take reasonable steps to notify another APP entity to which we disclosed the information of a correction unless impracticable or unlawful.

Who we may share personal information with

From time to time, we may share personal information with entities within and outside SFG and Integrity. We do this only where permitted by law and for the purposes explained in this policy. Depending on the product or service, recipients may include:

- a 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, AI service providers and paraplanners
- for corporate superannuation members, your employer or the employer's financial adviser
- lenders and other credit providers
- organisations within the Licensee, including related bodies corporate and authorised advice firms
- medical practitioners and health service providers, including pathology services
- companies involved in payment systems, including financial institutions, merchants and payment organisations
- organisations assisting with business functions, including auditors, compliance consultants, administration and back-office providers, direct marketing and technology support
- our solicitors and insurers, courts, tribunals and dispute resolution organisations
- other organisations that provide products or services to us or to you on our behalf
- any person to whom we or our service providers are required or authorised by law to disclose information, including law enforcement agencies and Australian or international government and regulatory authorities

We may disclose information with your consent, where you would reasonably expect the disclosure and it is related to the purpose for which we collected it, or where Australian law or another legal exception permits or requires disclosure. For sensitive information, the disclosure must be directly related to the collection purpose unless another exception applies.

If you ask us to deduct advice fees from your superannuation account, we may give the fund trustee a copy of the relevant Statement of Advice or Record of Advice and related fee documents so the trustee can confirm that the fee may be

charged under section 99FA of the Superannuation Industry (Supervision) Act 1993 and related trustee duties. We disclose only what the trustee needs for that purpose.

We may disclose personal information about our financial advisers to professional organisations, companies and consultants with whom we work.

We collect, use and disclose government-related identifiers only as permitted by law. These may include tax file numbers, Medicare numbers, driver licence numbers and passport numbers. We do not use them as our own client identifiers unless permitted by law. We handle tax file numbers in accordance with the Privacy (Tax File Number) Rule 2015 and relevant taxation, superannuation and personal assistance laws. You do not have to quote your tax file number. When we request it, we explain the legal basis and any consequences of not providing it. Please remove tax file numbers from documents where they are not required.

Where permitted by law, personal information may be used for direct marketing to promote events, products or services that may be relevant to you. You can opt out at any time, free of charge, by contacting us or using an unsubscribe facility in our messages. We act within a reasonable period and within five working days for commercial electronic messages. You may also ask us to stop sharing your information for another organisation's direct marketing and ask where we obtained your information. Sensitive information is used for direct marketing only with your consent. Electronic marketing and telemarketing must also comply with applicable spam and Do Not Call laws.

Disclosure of personal information overseas

Personal information may be disclosed to support services operating in countries including, but not limited to, the Philippines, India, Sri Lanka, the United Kingdom and the United States of America. Activities may include administration and back-office support, outsourced paraplanning, compliance assessments, direct marketing, software management and data storage.

When we share personal information with overseas recipients, we put appropriate data-handling and security arrangements in place and conduct regular due diligence on these providers.

Before disclosing personal information overseas, we take reasonable steps to ensure the recipient does not breach the Australian Privacy Principles unless a legal exception applies. We may remain accountable under Australian privacy law for the recipient's handling of the information. If we seek consent to a disclosure that would remove the protections under APP 8.1, we first explain this and its consequences and seek informed consent separately. This policy does not itself provide that consent. If an overseas disclosure is necessary for a service and you object, we will discuss available alternatives and explain any effect on the service. For health information, we also comply with applicable state and territory requirements for transfers outside the relevant jurisdiction.

Personal information may be stored in Australia or overseas. Australian storage does not prevent authorised overseas providers from accessing information. The overseas disclosure safeguards described above apply where required.

How we protect your personal information

We take reasonable technical and organisational measures to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure. These measures include appropriate staff procedures and security controls.

- educating staff and representatives about privacy, cybersecurity developments, threats and scams
- requiring passwords and appropriate access controls for systems
- regularly backing up client data and storing it securely
- using third-party providers, including financial planning software and storage providers, where appropriate
- using confidentiality arrangements that restrict unauthorised use or disclosure by third parties
- physical and electronic access controls for premises and systems
- firewalls, intrusion-prevention systems and virus-scanning tools
- secure networks and encryption for electronic data where appropriate
- secure storage for physical records and limits on physical access
- regular reviews of how data is stored and who can access it
- securely destroying or de-identifying information when it is no longer required and there is no legal obligation to retain it

We retain personal information for as long as needed for the purposes explained in this policy and to meet legal obligations. Different records have different retention periods. Relevant personal financial advice records must generally be kept for at least seven years after advice is given. Applicable customer due diligence records may need to be kept for at least seven years after the business relationship ends. Records may be kept longer where required by law or needed for a lawful purpose, such as resolving a complaint or legal claim. When information is no longer needed and is not legally required to be retained, we take reasonable steps to securely destroy it or ensure it is de-identified.

Cookies and other web technologies we use

Some personal information may be collected automatically while you navigate and interact with our websites. Electronic collection methods may include cookies, log files and web beacons.

Cookies are small files stored on your device that record information about your visit. We use cookies to improve your website experience, provide relevant information and manage access to parts of our websites. You can choose whether and how cookies are accepted through your browser settings, but this may affect access to some website features.

Web beacons are small pixel files that help us understand usage patterns, fix issues and improve products and services. Log files may contain information about devices and browsers used to access our websites and help diagnose problems, analyse trends and administer a site or mobile application.

Information collected electronically may include an IP address, screen size, device type, browser information, referring domain, pages visited, visit date and time, and geographic location at country level. We retain this information only as long as needed for a permitted purpose or as required by law. Where website tools disclose personal information to a service provider, the disclosure and overseas safeguards in this policy apply. We provide additional notices and obtain any consent required by law.

Notifiable data breaches

We assess suspected data breaches promptly and take reasonable steps to contain them and reduce harm. An eligible data breach generally involves unauthorised access to or disclosure of personal information likely to cause serious harm, or loss of information where unauthorised access or disclosure is likely and would be likely to cause serious harm. If remedial action prevents likely serious harm, notification may not be required. Where notification is required, we notify the OAIC and affected individuals as soon as practicable, or publish and publicise a notice where permitted by law.

If you receive a statement of an eligible data breach from us, please read and implement the recommended response steps.

Contacting us

If you have a question or concern about how your personal information has been collected, used or disclosed, please contact Sherpa Financial Group on 03 7047 9598 at Suite 1.02, 269 Centre Road, Bentleigh VIC 3204, or contact your adviser or the Integrity Compliance Manager using the details below.

Mail	Attention: Compliance Manager Suite 2, 1 Railway Crescent Croydon VIC 3136
Phone	(03) 9723 0522
Email	compliance@iplan.com.au
Website	www.iplan.com.au

Complaints about privacy

If you have a complaint about how your information has been handled, believe we have breached the Australian Privacy Principles, or disagree with a decision made under this policy, please contact us using the details above. Privacy complaints are free.

We aim to acknowledge a complaint within one business day or as soon as practicable. We investigate and generally provide a written response within 30 calendar days. If exceptional circumstances mean we cannot respond within that

period, we will write before the deadline, explain the delay and tell you about your right to complain to the Australian Financial Complaints Authority (AFCA), where applicable, and how to contact it. You may also contact the OAIC.

If you are not satisfied with our response, or we have not responded within 30 calendar days, you may complain to the OAIC. The OAIC generally asks that you complain to us first. You may also contact AFCA, of which Integrity is a member, where the complaint falls within its jurisdiction. Both services are free to consumers.

AFCA	Australian Financial Complaints Authority GPO Box 3, Melbourne VIC 3001 1800 931 678 | info@afca.org.au | www.afca.org.au
OAIC	Office of the Australian Information Commissioner GPO Box 5218, Sydney NSW 2001 1300 363 992 | enquiries@oaic.gov.au | www.oaic.gov.au

About this policy

We may amend or update this Privacy Policy as required by law or as our business processes or technology change. The current policy will be posted on www.sherpafg.com.au. We encourage you to check our website from time to time or contact us for a printed copy.

The information in this document is considered true and correct at the date of publication. Changes in circumstances after publication may affect its accuracy.