



Privacy Policy

Integrity Financial Planners Pty Ltd

ACN 069 537 855
AFSL No. 225051
Suite 2, 1 Railway Crescent
CROYDON VIC 3136

Version 3.0
Date Effective: 29th October 2026

Integrity Financial Planners Pty Ltd Privacy Policy

At Integrity Financial Planners Pty Ltd (Integrity), 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 document provides information and details about how we manage the personal information that we collect, hold, use and disclose about individuals. This Privacy Policy applies to Integrity, its employees and its representatives. We are bound by and abide by the Australian Privacy Principles established under the Privacy Act 1988 (Cth), as amended. A summary of the Australian Privacy Principles is available on the website of the Office of the Australian Information Commissioner (OAIC) at www.oaic.gov.au. We manage and protect your personal information in accordance with the Australian Privacy Principles.

This Privacy Policy is provided to you free of charge upon your request and is readily available through our website www.iplan.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

Integrity Financial Planners is a privately owned Australian Financial Services Licensee (AFSL) established in 1995 in Melbourne, Victoria. We have no ownership ties to any fund manager or financial institution. We provide licensing solutions to a group of like-minded advisers who operate professional financial planning practices that truly focus on improving the financial well-being and lifestyle of their clients.

When we refer to Integrity throughout this document, we mean Integrity Financial Planners Pty Ltd and its authorised representatives, including corporate authorised representatives, when acting on our behalf. Details of our current representatives can be found at www.iplan.com.au. A representative may also have a privacy policy for its own business 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 you with 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 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 interest to you

We collect, use, hold and sometimes disclose personal information about financial advisers and other people who we do business with (including employees) in order to administer and manage our business operations. This information is afforded the same standard of care as that of our clients.

What personal information we collect

We ask people for a range of personal information to assist us in providing relevant advice, products and services. The information we collect could include (but is not limited to) your name, date of birth, contact details, financial information, employment details, residency and citizenship status. We may also collect the personal information of your 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 also collect sensitive information about your medical history and your 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 interactive tool, such as a budget planner
- > provide documentation to us
- > when you communicate with us in person, over the telephone, fax, email, internet or by using other electronic devices

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 include:

- > a financial adviser
- > a mortgage broker or other credit representative
- > other professionals who act on your behalf, such as a lawyer or accountant
- > health professionals
- > indirectly from other organisations, who jointly with us, provide products or services to you e.g. fund managers, superannuation funds, life insurance companies and other product issuers once you have authorised us to obtain such information or authorised these other parties to provide us with this information
- > social media and publicly available sites

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 it is lawful and reasonable to do so. We take reasonable steps to tell people about our collection of their information at or before collection, or as soon as practicable afterwards.

It is your choice whether to provide your personal information. You have the right to not provide personal information, including about your identity. However, in this case, your adviser will warn you about the possible consequences and how this may impact on the quality of the advice provided. Your adviser may also decline to provide advice if they feel they have insufficient information to proceed. In some instances, we will decline to provide services or advice if we feel we have insufficient information for the scope of the service or advice requested.

Further, in some circumstances the law requires us to obtain and verify details of photographic and non-photographic identification documents.

You can deal with us anonymously or use a pseudonym (a name other than your own), unless the law requires or authorises us to identify you or it is impracticable to deal with you that way. For example, you can make a general enquiry without identifying yourself, 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 help with administrative tasks and functions such as prepare or summarising meeting notes. This can involve processing information discussed in meetings, including personal and, where relevant, health information. Before using a tool to record or transcribe a meeting, we will seek your agreement. We check 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 our 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 any legal limits. The 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. In accordance with the Australian Privacy Principles, we may not provide you with access to your personal information if:

- > we may reasonably believe providing access would pose serious threat to the life, health or safety of a person, or to public health or public safety;
- > providing access would have an unreasonable impact on the privacy of others;
- > the request for access would have an unreasonable impact on the privacy of others;
- > the request of access is frivolous or vexatious;
- > the information relates to existing or anticipated legal proceedings between us and would not be discoverable in those proceedings;
- > providing access would reveal our intentions in relation to negotiations with you in such a way as to prejudice those negotiations;
- > providing access would be unlawful;
- > denying access is required or authorized by or under Australian law or by court/tribunal order;
- > Integrity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to its functions or activities has been, is being, or may be engaged in, and giving access would be likely to prejudice the taking of appropriate action in relation to the matter;
- > providing access would be likely to prejudice enforcement-related activities conducted by, or on behalf of, an enforcement body; or
- > providing access would reveal evaluative information generated within Integrity in conjunction with a commercially sensitive decision-making process.

If we refuse access, or access in the way you requested, we will give you 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 will respond to access and correction requests within a reasonable period, generally within 30 calendar days. We will provide access in the way you request if it is reasonable and practicable. If your request is urgent, please indicate this clearly.

You can ask us to update your personal information. In most cases, you can update your personal information over the phone, or electronically via email to us or to your adviser. 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 give you written reasons (unless it would be unreasonable to do so), explain how to complain and, if you ask, take reasonable steps to attach a statement of your concern to the information. If you ask, we will take reasonable steps to notify another APP entity to which we disclosed the information of a correction, unless this is impracticable or unlawful.

Who we may share personal information with

From time to time we may share your personal information with other entities both within and outside Integrity. We do this only where permitted by law and for the purposes explained in this policy. Recipients 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, AI service providers and paraplanners
- > for corporate superannuation members, your employer or your employer's financial adviser
- > lenders and other credit providers
- > 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, administration and back office providers, direct marketing, 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 disclose your information with your consent, or where you would reasonably expect the disclosure and it is related to the purpose for which we collected it (directly related for sensitive information). We may also disclose information where Australian law or another applicable legal exception permits or requires it. For example, if you ask us to deduct advice fees from your superannuation account, we may give the trustee of that fund a copy of your relevant Statement of Advice or Record of Advice document and related fee documents. We do this so the trustee can confirm that the fee may be charged under section 99FA of the Superannuation Industry (Supervision) Act 1993 and the trustee's related duties. We will only disclose what the trustee needs for that purpose.

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

We collect, use and disclose government-related identifiers only as permitted by law. These include tax file numbers, Medicare numbers, driver licence numbers and passport numbers. We do not use them as our own client identifiers unless the law permits this. 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 will explain the legal basis and any consequences of not providing it. Please remove tax file numbers from documents we do not need them on.

Personal information collected may also be used, where permitted by law, for direct marketing purposes to promote events, products or services that may be of relevance to you. Please contact us should you wish not to receive direct marketing. You can opt out at any time, free of charge, by contacting us or using the unsubscribe facility in our messages. We will 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. We will respond as the law requires. We use sensitive information for direct marketing only with your consent. Our electronic marketing and telemarketing must also comply with applicable spam and Do Not Call laws.

Disclosure of personal information overseas

Your personal information may be disclosed to support services operating from countries including, but not limited to, the Philippines, India, the United Kingdom and the United States of America for activities and processes such as administration and back-office support, paraplanning, compliance assessments, direct marketing, software management or data storage.

When we share your personal information with overseas recipients, we make sure appropriate data handling and security arrangements are in place and we 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 that information. If we seek your consent to a disclosure that would remove these protections under APP 8.1, we will first explain this and its consequences and seek your 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 any available alternatives and explain any effect on the service. For health information, we also comply with applicable state and territory requirements for transfers outside that jurisdiction.

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

How we protect your personal information

We strive to ensure that the personal information you provide to us is stored safely and securely. We take numerous precautions to protect the personal information we hold about you from misuse, interference and loss, and from unauthorised access, modification or disclosure. We take reasonable technical and organisational measures to protect information, including appropriate staff procedures and security controls.

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
- > requiring our staff and representatives to use passwords when accessing our systems
- > client data is backed up regularly and stored securely
- > client data may be stored with a third party provider eg financial planning software; storage provider etc
- > where appropriate, using strict confidentiality arrangements restricting third parties' use or disclosure of personal information for any unauthorised purposes
- > employing physical and electronic means, including access controls (as required) to protect against unauthorised access to buildings
- > employing firewalls, intrusion prevention systems and virus scanning tools to protect against unauthorised persons, malware and viruses from entering our systems
- > some of the systems we use are on dedicated secure networks or transmit electronic data via encryption

- > providing secure storage for physical records, securing paper files in locked cabinets/rooms and limiting physical access to authorised personnel only
- > the manner in which your data is stored is regularly reviewed to ensure it is stored securely and only authorised persons are able to access your data
- > where personal information is no longer required, we take steps to de-identify or destroy the information in a secure manner

We keep 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. For example, relevant personal financial advice records must generally be kept for at least seven years after the 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 need to 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 we are not legally required to retain it, 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, whilst navigating through and interacting with the content of our websites. The electronic methods of collection we may use include cookies, log files and web beacons.

Cookies are small files stored on your device that record information about your visit to our websites. We use cookies 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 are small pixel files that 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 may 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.

The information we collect by these electronic means 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 retain this information only for 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 any 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 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 the law allows.

If you receive a statement of an eligible data breach from us, you should read and implement the steps that are recommended to you in response to the eligible data breach.

Contacting us

If you have any queries or are concerned about how your personal information has been collected, used or disclosed, please contact the Compliance Manager on the information 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

Though we always try to do our best, sometimes things may go wrong. If you have a complaint about the way your information has been handled or concerns about the privacy of your information, believe we have breached the APPs or disagree with a decision that we have made in relation to our Privacy Policy, please let us know. We would greatly appreciate the opportunity to fix the problem for you and identify if there is something that we can do better in the future. Making a complaint regarding your privacy is free for everyone. Simply contact us via the details listed above.

We aim to acknowledge your complaint within one business day or as soon as practicable. We will investigate and generally provide a written response within 30 calendar days of receiving your complaint. If exceptional circumstances mean we cannot respond within that time, we will write to you before the deadline, explain the delay and tell you about your right to complain to AFCA, where applicable, and how to contact it. You may also contact the OAIC as explained below.

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

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

	Office of the Australian Information Commissioner
Mail	GPO Box 5218 Sydney NSW 2001
Phone	1300 363 992
Email	enquiries@oaic.gov.au
Website	www.oaic.gov.au

About this policy

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

The information in this document is considered to be true and correct at the date of publication. Changes to circumstances after the time of publication may impact on the accuracy of the information held.