Privacy Policy

Integrity Financial Planners Pty Ltd

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

Version 2.0
Date Effective: 15th October 2020

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 and the Privacy Amendment (Privacy Enhancement) Act, 2012. A summary of the Australian Privacy Principles is available on the website of the Office of the Australian Information Commission www.oaic.gov.au. We manage and protect your personal information in accordance with the Australian Privacy Principles.

As a Registered Tax (Financial) Adviser, Integrity and it's representatives are also bound by item 6 of the Code of Professional Conduct under the Tax Agent Services Act 2009 (section 30-10) which prohibits us from disclosing any information relating to your affairs to a third party without your prior permission.

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

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 are referring to all financial planners (authorised representatives and Corporate authorised representatives) appointed under our AFSL on the date that you are reading this Privacy Policy. Details of our current authorised representatives and corporate authorised representatives is continuously updated and can be found on the Integrity website at www.iplan.com.au.

Why we collect and use personal information

As a financial planning organisation, we are subject to certain legislative and regulatory requirements (including but not limited to the Corporations Act 2001, Tax Agent Services Act 2009, Anti-Money Laundering and Counter-Terrorism Financing Act 2006, Financial Adviser Standards and Ethics Authority (FASEA)) 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 collect, hold, use and disclose personal information so we can provide you with financial products, advice and services relevant to your needs. 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 may also collect sensitive information about your medical history and your health and lifestyle to provide financial advice about life insurance products. 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

Situations where we may collect personal information about you from other people and organisations, with your consent include (but are not limited to):

- 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

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 have the right to interact anonymously or under a pseudonym. However, it is impracticable for Integrity to deal with individuals who have not identified themselves or who have used a pseudonym. Integrity only allows individuals not to be identified, or to use a pseudonym, when requesting publicly available information; e.g. requesting for Integrity's postal address.

Accessing and updating personal information

You can request access to personal information we hold about you. There may be a cost involved with locating, copying or sending you the information you request. The cost will be discussed and agreed with you at the time.

There may be circumstances where we refuse to provide you with the information you request, for example when the information is commercially sensitive. In accordance with the Australian Privacy Principles, we may not provide you with access to your personal information if:

- providing access would pose a serious threat to the life or health of a person or the health and safety of the public;
- providing access would have an unreasonable impact on the privacy of others;

- the request for access is frivolous or vexatious;
- the information related 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 authorised 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 is likely to prejudice actions being conducted by an enforcement agency; or
- providing access would reveal evaluative information generated within Integrity in conjunction with a commercially sensitive decision-making process.

In the event we refuse your request to access to your personal information; we will provide you with a written explanation for that refusal.

We will endeavour to respond to any request for access within 14-30 days depending on the complexity of the information and/or the request. If your request is urgent, please indicate this clearly.

We will update your personal information if you contact us. In most cases, you can update your personal information over the phone, or electronically via email to us or to your adviser.

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. This will 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 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, direct marketing, client experience surveys, debt recovery and information and communication 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 also disclose your information to a third party where you have given your consent or where you would reasonably expect us to disclose your information to that third party.

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

The only circumstances in which we would collect, use or disclose your government related identifiers is where we are required or authorised by law to do so. For example, we may be required to disclose your Tax

File Number (TFN) to the Australian Taxation Office, a superannuation or retirement income product provider. Likewise, we may need to disclose your Medicare number to Centrelink in order to assess your social security eligibility. A copy of your Drivers licence and / or passport may also be collected when we are required to verify your identity.

Personal information collected may also be used 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.

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 paraplanning, compliance assessments, direct marketing, software management or data storage.

When we share your personal information to overseas recipients, we make sure appropriate data handling and security arrangements are in place and we conduct regular due diligence on these providers.

When transferring information to foreign jurisdictions, we will ensure that we satisfy the following:

- we will take reasonable steps to ensure the overseas recipient does not breach the APPs in relation to the information;
- we form a reasonable belief that the overseas recipient is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the APP protect the information and there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or
- we will seek your informed consent prior to disclosing your information overseas. Most of the services that we provide are based on an integrated model of professional and reliable service providers that we have selected after thorough due diligence. If you do not agree to us disclosing your information outside Australia to our external service providers, we will not be able to provide services to you.

Personal information is generally hosted on servers located in Australia. If you access our services from outside Australia, you consent to the transfer of your personal information to your overseas location which may be a jurisdiction that may not provide the same high level of protection we apply in Australia.

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 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

In the event you stop being a client of Integrity (or a subsidiary), any personal information which we hold about you will be maintained securely for a period of at least 7 years after you cease being a client of Integrity, in order to comply with legislative requirements.

Cookies and other web technologies we use

Some personal information may be collected automatically, without your knowledge, 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 a small text or pixel file stored on your device that records 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 is generally not stored for long – they are temporary records – and 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).

Notifiable data breaches

We are required to notify you and the Information Commissioner of an eligible data breach. An eligible data breach happens if:

- there is unauthorised access to, unauthorised disclosure of, or loss of personal information held by us; and
- the access, disclosure or loss is likely to result in serious harm to you.

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 all of our clients. Simply contact us via the details listed above.

In order to resolve the issue as easily and simply as possible, we ask that you follow the process below:

1. Collect of all the information that you have about the issue and think about how you believe is the best way for us to resolve this issue for you;
2. Contact your financial planner and let them know what has happened; why it is an issue for you; how it has affected you and how you would like the issue to be resolved. Your financial planner will be able to review the situation for you and if possible, resolve it quickly.

If your financial planner is unable to resolve the issue for you or to your satisfaction, please contact the Integrity Compliance Manager using the above contact information. Our aim is to resolve all issues and complaints as soon as we can. We will investigate your issues or complaint and respond to you within 45 days. Some complex matters may require an extension to thoroughly investigate the complaint and bring it to resolution.

If you are not fully satisfied with our response, you can contact the Australian Financial Complaints Authority (AFCA), an external dispute resolution body of which Integrity is a member, or the Office of the Australian Information Commissioner (OAIC) as detailed below:

	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.