FIRST light.

FINANCIAL PLANNING

Privacy policy.

Firstlight Financial Planning Pty Ltd · ABN 81 618 516 135 · AFSL 532193
11/76 Township Drive, Burleigh Heads QLD 4220
(07) 3132 8977 · clients@firstlightfp.com.au
www.firstlightfinancialplanning.com.au

EFFECTIVE DECEMBER 2026



Privacy policy.

Firstlight Financial Planning is committed to keeping your personal information confidential and secure.

This policy explains the kinds of personal information we collect and hold, how and why we collect, 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 and prospective clients, and to others we deal with — including our clients' family members, beneficiaries and representatives, and our own advisers, employees, contractors, suppliers and job applicants.

"Firstlight Financial Planning", "Firstlight", "we" and "us" mean all staff, representatives and associated entities of Firstlight Financial Planning Pty Ltd (ABN 81 618 516 135, AFSL 532193). The associated entities include Firstlight Business Insurance Pty Ltd (ABN 93 632 331 527), together the "Firstlight Group". Given how closely these entities work together, this policy also covers information shared between them and their representatives.

We may also give you a collection notice for a particular product, service, website or activity. Where that notice is more specific than this policy, the notice applies to that activity, to the extent of any difference.

Australian Privacy Principles

Firstlight handles personal information in line with the Privacy Act 1988 (Cth), including the Australian Privacy Principles (APPs) and the Notifiable Data Breaches scheme, and other laws that apply to us. We will be open with you about how we use it.

Key terms

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

Sensitive information is a special category of personal information. It includes health and genetic information, biometric information used to identify you, racial or ethnic origin, political opinions, religious or philosophical beliefs, sexual orientation or practices, criminal record, and membership of a political, professional or trade association or trade union.

Government-related identifiers are numbers issued by government to identify you, such as a tax file number, Medicare number, passport number or driver licence number.

The information we may collect.

As a provider of financial services we are subject to legislative and regulatory requirements that oblige us to obtain and hold detailed information that personally identifies you. What we collect depends on our relationship with you and the services involved. It may include:

- identity details, such as your name, address, date of birth, gender, citizenship and residency status, photographs and identity documents;
- contact details and communication preferences;
- family and relationship information, such as your marital status, dependants, beneficiaries and estate planning arrangements;
- employment, occupation and education details;
- financial information, such as your income, expenses, assets and liabilities, current investments, superannuation, bank account details, tax information and transaction history;
- advice information, such as your goals, needs, priorities, risk profile and preferences, and records of the advice we give and the instructions you give us;
- health, medical, lifestyle, insurance and claims information, where relevant to insurance advice, applications or claims;
- government-related identifiers, such as tax file numbers, where the law requires or authorises us to collect them;
- records of meetings, calls, correspondence, complaints, consents and other dealings with us;
- online and technical information, such as your IP address, device and browser details, log-in activity, cookies, pages visited and form submissions; and
- information about our advisers, representatives, employees, contractors, suppliers and job applicants.

Health and other sensitive information

We only collect sensitive information when it is reasonably necessary for our services and you consent, or where the law otherwise permits or requires it. For example, we may collect health and lifestyle information so that we can advise you on insurance and help with applications, underwriting

or claims. We will only disclose it where that is necessary to help you apply for or manage a financial product or claim, or where the law requires it.

Information about other people

If you give us personal information about someone else — such as your partner, a dependant or a beneficiary — please make sure you are authorised to do so, and let them know about this policy unless that would be unreasonable or impracticable.

How we collect information

Wherever practicable we collect information from you personally — for example, when you meet or speak with us; complete a fact find, application, identity check or other form; use our website, client portal or online tools; or send us emails, messages or documents.

We may also collect it from other sources where you consent, where you would reasonably expect us to, or where the law permits. These include your other professional advisers (such as your accountant or solicitor), people authorised to act for you, product issuers, insurers, superannuation funds, employers, health professionals, identity verification services, referrers, public registers and our service providers.

Information we didn’t ask for

If we receive personal information we did not ask for, we check whether we could have collected it under the APPs. If we could not, we destroy or de-identify it, where it is lawful and reasonable to do so.

Anonymity

You can deal with us anonymously or using a pseudonym where that is lawful and practicable — for a general enquiry, for example. But financial services do not lend themselves to anonymous clients. To give you personal advice or arrange a financial product, we need to know who you are, and we need full and accurate information about you.

Why we collect and hold personal information.

Understanding your financial position, and helping you improve it, is the whole job. We collect, hold, use and disclose personal information where it is reasonably necessary to:

- provide financial advice and related services — including preparing, implementing and reviewing your advice;
- understand your needs, objectives and financial circumstances, and assess whether products and services are suitable for you;
- arrange, administer and manage your investments, superannuation, insurance and other financial products;
- verify your identity and meet our legal obligations, including taxation, anti-money laundering and counter-terrorism financing, sanctions and record-keeping requirements;
- communicate with you and manage our relationship, including fees, payments and service arrangements;
- marketing material to keep you informed about what we offer, or provide you with general information (see “Direct marketing”);
- handle enquiries, complaints, disputes, claims and legal proceedings;
- prevent, detect and investigate fraud, cyber incidents and other unlawful activity or misconduct;
- carry out compliance reviews, audits, quality assurance, training, data analysis and business planning;
- manage our advisers, representatives, employees, contractors and suppliers;
- protect our legal rights — including our copyright and trade marks — and those of our clients and others;
- facilitate a proposed or completed sale, transfer or restructure of our business, subject to confidentiality and legal requirements; and
- carry out any other purpose we tell you about, or that you authorise.

If you don’t provide information

You don’t have to give us all the information we ask for. But if information is incomplete, inaccurate or not provided, we may not be able to verify your identity, give you appropriate advice, arrange a product or service, or continue working with you.

Use and disclosure of collected information.

We use the personal information we hold to provide products and services to you, including financial advice and investment management. We use and disclose it for the main purpose for which we collected it; for a related purpose you would reasonably expect (or, for sensitive information, a directly related purpose); with your consent; or where the law requires or authorises it.

In some cases we need to disclose personal information to organisations outside the Firstlight Group. Depending on the circumstances, these may include:

- regulators such as the Australian Transaction Reports and Analysis Centre (AUSTRAC), the Australian Securities and Investments Commission (ASIC), the Australian Taxation Office (ATO) and the Australian Prudential Regulation Authority (APRA), and other government agencies, law enforcement bodies, courts, tribunals and external dispute resolution bodies, where required or authorised;
- financial institutions, for the provision of financial products such as investments, superannuation and insurance — including platform operators, superannuation trustees, fund managers, insurers, banks and stockbrokers;
- your adviser or advisers;
- organisations providing research, technical (tax, legal and similar), paraplanning or administration services;
- organisations we contract with to provide us with a service, such as software, cloud hosting, cybersecurity, identity verification, mailing, printing and archiving providers;
- professional advisers such as accountants, solicitors, auditors, compliance consultants and medical practitioners;
- people acting for you, such as an attorney, guardian, executor, trustee, accountant or solicitor; and
- any party acquiring an interest in our business, under an agreement to maintain confidentiality and to the extent the law permits.

Where our service providers can see your personal information, we require them to keep it confidential and to have appropriate privacy policies and procedures of their own. We do not sell personal information. For analysis and product development, we de-identify your data.

Direct marketing

From time to time we may use your contact details to send you information about products, services, events or insights we think will be of interest, where the law permits. We won't use sensitive information for marketing unless you consent. You can tell us to stop at any time — use the unsubscribe link in our emails, or contact us by phone or in writing (see "Queries and complaints"). We will act on your request within a reasonable time and won't charge you. You can also ask us where we obtained the information we used.

Government-related identifiers

We only collect, use or disclose government-related identifiers, such as a tax file number or Medicare number, where the law requires or authorises it or the APPs otherwise permit it. We will not adopt any of them as our own way of identifying you. We handle tax file numbers in line with the Privacy (Tax File Number) Rule 2015.

Overseas disclosure.

Some of our service providers are located outside Australia, or store or access information from overseas — for example, for paraplanning, administration, software, cloud hosting, cybersecurity, artificial intelligence (AI) tools, technical support and data processing. This means your personal information may be disclosed to, stored in, or accessed from other countries.

The countries in which these recipients are likely to be located include **the Philippines**.

Before we disclose personal information overseas, we take reasonable steps to make sure the recipient handles it consistently with the APPs, unless an exception under the Privacy Act applies. Overseas recipients may be subject to different privacy laws, and foreign governments, courts or law enforcement bodies may be able to access information under those laws.

Automated decisions and AI.

We use software, including AI tools, to help us work efficiently and accurately — for example, to verify identity, prepare documents, record and summarise meetings, keep file notes, triage enquiries and review the quality of our work. These tools support our people; they don't replace them. A Firstlight adviser or staff member remains responsible for the advice and services we provide, and we apply human review and other controls where appropriate.

Decisions that may significantly affect you

The Privacy Act requires us to tell you if we arrange for a computer program to use your personal information to make a decision — or to do something substantially and directly related to making a decision — that could reasonably be expected to significantly affect your rights or interests.

Decisions made solely by a computer program

We do not make any decisions that could significantly affect your rights or interests solely by the operation of a computer program. A person is always involved in making those decisions.

Decisions a computer program helps us make

We use computer programs to do things that are substantially and directly related to the following kinds of decisions:

- **Whether we can accept you as a client.** Electronic identity verification and screening tools check your identity details and documents against official and commercial sources, and against sanctions and politically exposed person lists, as part of our anti-money laundering and counter-terrorism financing obligations. A staff member reviews any result that does not verify, or that flags a possible match.
- **The investment risk profile we recommend for you.** Risk profiling tools score your answers to our risk profile questionnaire and suggest a risk profile, which your adviser discusses and confirms with you.
- **The strategies and products we recommend.** Financial modelling, research and comparison tools — such as cashflow, retirement, superannuation and insurance needs calculators, and product and insurance quoting tools — produce projections, calculations and comparisons that your adviser relies on in forming advice recommendations.

Kinds of personal information used

Depending on the decision, these programs may use:

- identity details and documents, such as your name, date of birth, address and driver licence or passport details;
- your answers to our risk profile questionnaire, and your goals, needs and investment preferences;
- financial information, such as your income, expenses, assets, liabilities, superannuation, investments and tax position;
- personal and family circumstances, such as your age, relationship status, dependants, occupation and employment; and
- health and lifestyle details, such as smoker status, where relevant to insurance needs analysis, quotes and comparisons. This is sensitive information.

Product issuers and insurers may use their own automated systems when assessing your applications and claims. Their privacy policies explain how they do so.

How we manage AI tools

If personal or confidential information is made available to an AI tool, we only use providers we have assessed and approved. We do not allow personal or confidential information to be shared with public AI models, or with any AI service that may use that information to train large language models.

If you have a question about how technology was used in a decision about you, contact our Privacy Officer (see “Queries and complaints”).

Keeping your information secure.

The security of your personal information matters to us. It is held in secure, cloud-based client management and document management systems — including systems operated by our service providers — and in any paper records, which we store securely. We take reasonable steps, including technical and organisational measures, to protect it from misuse, interference and loss, and from unauthorised access, modification or disclosure. These include:

- access controls that limit information to the people who need it;
- multi-factor authentication and secure client portals;
- encryption and secure transmission where appropriate;
- firewalls, malware protection, monitoring, software updates and backups;
- physical security for our offices and paper records;
- staff and representative training, confidentiality obligations and incident reporting;
- due diligence on our service providers, and contracts requiring them to protect your information; and
- cyber incident and data breach response procedures.

How long we keep it

The law requires us to keep your personal information for a certain period — generally at least seven years. Once we no longer need it for any purpose and are not required to keep it, we destroy it by secure means or permanently de-identify it.

Data quality

We aim to keep the information we hold about you accurate, complete, up to date and relevant. If at any stage you believe it is wrong or incomplete, please contact us (see “Accessing and correcting your information”).

Data breaches

We have procedures to identify, contain, assess and respond to suspected data breaches. If we have reasonable grounds to believe an eligible data breach has occurred — one likely to result in serious harm — we will notify the people affected and the Office of the Australian Information Commissioner (OAIC), as the Notifiable Data Breaches scheme requires, including steps you can take in response.

Accessing and correcting your information.

You can ask to see the personal information we hold about you, and ask us to correct anything that is inaccurate, out of date, incomplete, irrelevant or misleading. To make a request, contact our Privacy Officer (see “Queries and complaints”). You don’t need to give a reason. We will ask you to identify yourself to our satisfaction, and may ask you to help us locate the information you want. We will then discuss how you would like to receive it.

There is no charge to make a request or to correct your information. We may charge a reasonable cost for giving you access, but we will tell you first. We aim to respond within 30 days.

In limited circumstances the law allows us to refuse access or correction. If we do, we will tell you why in writing (unless that would be unreasonable) and how you can complain. If we refuse to correct your information, you can ask us to attach a statement to it noting that you believe it is inaccurate, out of date, incomplete, irrelevant or misleading.

Your rights if you are in the EU

If the General Data Protection Regulation applies to our handling of your personal data, you have the right to access your data; to correct or rectify it; to delete it, subject to applicable law; to have it processed only in accordance with applicable law; to have copies of it moved to another controller; to object to our processing it otherwise than in accordance with the law; and to withdraw any consent to our processing it at any time. Email compliance@firstlightfp.com.au to exercise any of these rights.

Our website.

Cookies

When you visit our website, details may be recorded about your visit — such as the time and date, your IP address, device and browser type, the pages you view, how long you stay and the page that referred you. We use this information to operate and secure our website, understand how it is used, fix problems and improve our content. Where we use it for statistical purposes, we use it in a combined form that does not identify you.

We may use cookies to identify your browser, so that next time you visit we remember your log-in details and preferences. A cookie is a small file that stays on your computer and lets Firstlight Group websites recognise your browser. We may also use similar technologies, such as analytics tools and pixels, to understand how our website and communications perform. If you would rather not allow cookies, you can adjust your browser settings to reject them, or to notify you when they are being used — although some features may not work as well.

Information you submit through our online forms is handled in line with this policy.

Links to third-party websites

Firstlight Group websites may contain links to external websites that may benefit you. Those sites should have privacy statements of their own, and we recommend you read them. Third-party websites are not covered by this policy and are not subject to our privacy standards and procedures.

Queries and complaints.

If you want more information about this policy, want to access or correct your information, or believe we have breached your privacy or the APPs, please contact the Firstlight Financial Planning Privacy Officer using the details below. Please give us enough information to understand the issue and the outcome you are seeking.

We will acknowledge your complaint promptly, investigate it fairly, and aim to give you a written response within 30 calendar days. If we need more time, we will tell you why and when you can expect our response.

Privacy Officer	Firstlight Financial Planning Privacy Officer
Email	practiceadmin@firstlightfp.com.au
Phone	(07) 3132 8977
Post	11/76 Township Drive, Burleigh Heads QLD 4220
Licensee	Firstlight Financial Planning Pty Ltd · ABN 81 618 516 135 · AFSL 532193

If you are not satisfied with our response, you can contact:

Office of the Australian Information Commissioner (OAIC)

www.oaic.gov.au
1300 363 992
GPO Box 5288, Sydney NSW 2001

The OAIC requires complaints to be made in writing.

Australian Financial Complaints Authority (AFCA)

www.afca.org.au
info@afca.org.au
1800 931 678 (free call)
GPO Box 3, Melbourne VIC 3001

For complaints connected with our financial services. Time limits may apply.

Changes to this policy

We review this policy from time to time and may update it to reflect changes in the law, technology or how we handle personal information. The current version is always available free of charge on our website at www.firstlightfinancialplanning.com.au, and we can give you a copy in another form on request. This policy was last updated in December 2026.

FIRST light.

FINANCIAL PLANNING

Advice that starts with your life.

THE LICENCE

Firstlight Financial Planning Pty Ltd
AFSL: 532193
ABN: 81 618 516 135
11/76 Township Drive
Burleigh Heads QLD 4220

GET IN TOUCH

(07) 3132 8977
clients@firstlightfp.com.au
www.firstlightfinancialplanning.com.au