

Smart Financial Privacy Policy 06 July 2026

Smart Financial is committed to safeguarding the privacy of information provided to us and information about visitors to our website, apps and offices. This Privacy Policy explains how we may collect, use, hold and disclose information that we obtain about you, and your rights in relation to that information.

Your privacy is important to us

This privacy policy applies to the following entities:

- Smart Financial Capital Pty Ptd (ABN 78 627 468 759)
- Smart Financial Pty Ltd (ABN 99 126 697 229)
- Smart Financial Lending Pty Ltd (ABN 61 674 419 400)
- Smart Financial Accounting Pty Ltd (ABN 16 657 318 931)

References to “**Smart Financial**”, “**we**”, “**us**” or “**our**” throughout this document refer individually or collectively to the above entities.

This Policy is addressed to individuals outside of our organisation with whom we interact, including visitors to our offices (the locations of our offices can be found at <https://smartfinancial.com.au/location>, visitors to our website and any other associated websites under our control (together our “**websites**”), (together, “**you**”). Defined terms used in this Policy are explained in the Glossary at the end of this Policy.

This Policy may be amended or updated from time to time to reflect changes in our practices with respect to the handling of personal or sensitive information, or changes to applicable law. We encourage you to read this Policy carefully, and to regularly check this page to review any changes we might make to the terms of this Policy. All information about you which is held by us, will be governed by our most recent Policy.

Laws applicable to this Privacy Policy

We have obligations under the Privacy Act 1988 (**Cth**) (‘the **Privacy Act**’) and applicable state/territory privacy acts, to have a privacy policy, and to handle your personal information in accordance with the Australian Privacy Principles (**APPs**).

Collection of Personal Information

We collect personal information from you, through our interactions with you and as part of providing our services. The personal information we collect will depend on the context of your interactions with us, and the choices you make, including your communication preferences and the products and services you use. We may also obtain personal information about you from third parties.

The main way we collect personal information about you is when you give it directly to us (e.g. when you contact us), however we may also collect personal information:

- when you complete online forms on our website or via emails we send you;
- from product providers you hold when we are providing you with advice services;
- when you apply for a role or work placement opportunity;
- when you visit our website;
- when you attend a seminar that we may or other hosted events
- when you visit our offices;
- when you select communication preferences to receive publications and other marketing information (please see 'Direct Marketing' section for more information); and
- from other representatives, authorised by you to act on your behalf (e.g. financial adviser, your power of attorney, executors managing an estate);

We may also receive personal information about you from government agencies (i.e. the Australian Tax Office or law enforcement authorities).

If you choose not to provide the requested personal information, we may not be able to provide important services to you, for example being able to act in your best interests as your financial adviser.

Cookies and Similar Technologies

We may collect your personal information using Cookies and similar technologies. These are small files stored on your device (computer or mobile device).

Artificial Intelligence (AI) Tools

Artificial intelligence tools are used responsibly and ethically, solely to enhance efficiency by optimising and simplifying our processes, as well as supporting document generation. These digital tools enable us to focus our efforts on delivering the best possible financial outcomes for our clients. They are not intended to replace human intelligence or human resources.

Client data, including Personal Identifiable Information (PII) is handled securely, remains private, and is never shared with AI models or third parties.

'Claras AI' and 'Microsoft Copilot' are both tools that are approved for staff use, based on their alignment with Smart Financials data security, privacy, and confidentiality requirements. These tools have been assessed as providing an appropriate level of protection for personal and sensitive information, including safeguards relating to data handling, storage, and access controls.

As such, they may be used to support administrative and operational tasks, including but not limited to:

- Record our meetings for compliance and record-keeping purposes. These recordings will not be retained for more than 180 (one hundred and eighty) days;
- Generate structured file notes;
- Update and/or generate advice documents and supporting administrative templates (e.g., Records of Advice – ROAs or Statements of Advice - SOAs);
- Email preparation;
- Other internal communications.

Types of Personal Information Collected

We may collect and hold a range of personal information about you. This may include, but is not limited to:

- name, address, date of birth and contact details;
- Tax File Number (TFN);
- employment details and employment history;
- financial information such as bank balance, superannuation balance, assets, liabilities, investments, insurance, income and expenditure;
- payment information including bank account and credit card details;
- information about your family corporate structure, such as entities or any trusts, including beneficiaries and settlors;
- information about your family commitments and social security eligibility and entitlements;
- details of your financial circumstances and objectives including your risk tolerance;
- information about your beneficiaries; and
- details about your citizenship, residency or visa status.

Collection of Sensitive Information

Sometimes we may need to collect sensitive information about you, for example, to arrange an insurance policy or claim, or to handle a complaint. Some of this information may be collected from you and provided to our insurers. If required, we may obtain independent medical reports directly from your medical practitioner(s).

Use of Personal Information

We may use your personal information to carry out our functions or activities or to provide you with a product or service, including to:

- establish and administer the financial and superannuation products and services (including insurance cover) that you acquire from or through us;
- facilitate our internal review procedures;
- provide you with financial planning advice and related services, including the preparation of advice documents and implementation documents (i.e. in order to implement financial planning recommendations for you);
- provide you with promotional information and services about us;
- conduct identity verification;
- conduct pre and ongoing employment background checks;
- directly market our products and services to you; including through social media and other digital platforms;
- undertake market research*, member/client satisfaction surveys and member/client data analysis;
- improve our products and services; and
- comply with all applicable laws and obligations as part of the Financial Advice Association of Australia (FAAA).

If you apply for a job with us, we will collect your information for recruitment purposes, to manage your application and your ongoing employment.

**Due to the nature of our business, it is difficult for us to deal with you anonymously and to do so may restrict the range of products and services we can offer you. On some occasions (such as participating in a market survey), you may have the option to deal with us anonymously or use a pseudonym.*

Disclosure of Personal Information

We may disclose your personal information to third parties for legitimate business purposes (including operating our website and providing products and services to you), if you have consented to it, or if we are permitted to do so by law, and we will do so in accordance with applicable law and subject to applicable regulatory requirements. This includes, but is not limited to:

- our related entities;
- financial institutions, payroll platforms, clearing houses;
- our legal advisers and auditors;
- employers or former employers (non-sensitive information only);
- legal or regulatory authorities;

- our service providers (such as providers of data hosting or warehousing services and document review services);
- any party you have authorised to act on your behalf (such as your power of attorney, trustee or financial adviser);
- any relevant medical, health and wellbeing professionals in connection with an insurance claim and our insurer;
- government agencies (such as Centrelink, WorkCover, ATO, Department of Veterans' Affairs);
- international agencies with your consent (such as a KiwiSaver fund);
- other organisations or super funds (such as your employer, other super funds where you are transferring into or out of a superannuation fund);
- any relevant party, law enforcement agency or court, as required by law (such as your spouse or former spouse as required by a court order under the Family Law Act 1975 (**Cth**));
- any relevant third-party acquirer(s), in the event that we sell or transfer all or any portion of our business or assets (including in the event of a reorganisation, dissolution or liquidation); and
- any relevant third-party provider, where our use third party advertising, plugins or content.

We recommend that you review that third party's privacy policy before interacting with its advertising, plugins, or content.

Direct Marketing

We may use your personal information to send you direct marketing communications and information about our services and products, in accordance with the Spam Act, Do Not Call Register Act and the Privacy Act.

If we use or disclose your sensitive information for the purpose of direct marketing, we would only do so with your express consent.

We engage third party service providers to assist us with delivering direct marketing via various channels, including through social media and other digital platforms. We take all reasonable steps to ensure that your personal information is protected when disclosing information to such third parties.

Sometimes, we may de-identify your information before disclosing it to third parties to facilitate our marketing activities.

You may opt-out of receiving direct marketing communications by contacting us using the details provided in this Policy or by using the relevant opt-out facilities provided in each communication (e.g. an unsubscribe link).

Holding Personal Information

We may hold personal information in hard copy and electronic formats, including cloud storage. We aim to keep the personal information only for as long as we need it for business or legal reasons. In accordance with the law, you can withdraw your consent to us holding your personal information at any time.

Storing personal information overseas

In some cases, we engage third parties to host electronic data (including data in relation to the services we provide) on our behalf. These data warehouses may be located overseas, however at the time of this policy all customer data is housed in Australia. These data warehouses will have in place appropriate security and privacy protocols to comply with the Privacy Act and the Australian Privacy Principles.

We do employ administration staff in the Philippines. All data is retained and managed within the Smart Financial network and adheres to the terms of this privacy policy.

Security

We take security measures to protect the personal information we hold from misuse, interference and loss, and from unauthorised access, modification or disclosure. These include physical (for example, security passes to enter our offices and storage of files in lockable cabinets) and technology (for example, restriction of access, firewalls, the use of encryption, user logons, passwords, biometric authentication and digital certificates) security measures.

If you visit an unsecured area of our public website, that does not require log in details, we will not collect or retain your personal information. If you complete any forms on the public website, we will retain your contact information securely.

Users can play an important role in the security of their information by keeping their user logins and passwords to their online accounts and our mobile applications confidential and ensuring their biometric identifier for authentication used to access the mobile applications is the only identifier stored on their mobile devices. We encourage you to be vigilant about the protection of your own personal information when using third party digital services (such as social media platforms).

As far as reasonably practicable, we will make sure that our relationships with third parties include appropriate protection of your privacy.

Data breaches

We may need to notify the Office of the Australian Information Commissioner (OAIC) and affected individuals if we become aware of an eligible data breach. We have policies and procedures in place to identify and assess data breaches and to notify the OAIC if required.

Your legal rights to access and correct your information

The privacy laws of some jurisdictions may give you a number of rights including:

- the right not to provide your personal information to us;
- the right of access to your personal information;
- the right to request rectification of inaccuracies in your personal information;
- the right to object to the processing of your personal information;
- the right to have your personal information transferred to a third party;
- the right to withdraw your consent; and
- the right to lodge complaints.

We may require proof of identity before we can give effect to your exercise of any of these rights.

If you would like to request a copy of the personal information we hold about you, or would like to take steps to exercise any of your other rights, please contact us in writing as set in the section below. We may decline in some circumstances to provide access and may charge a fee for access if the relevant legislation allows us to do so.

Information we hold about you should be kept up-to-date and accurate. Please advise us in writing of any changes to your information using the 'Contact Details' set out below.

Enquiries and complaints

If you have any comments, questions or concerns about data privacy or would like to make a complaint about a breach of your privacy, please contact us via any of the below:

Warilla (Head Office)

A: Level 1

162-172 Shellharbour Road

Warilla NSW 2528

P: (02) 42953331

E: compliance@smartfinancial.com.au

Nowra

A: 51 Bridge Street

Nowra NSW 2541

P: (02) 42953331

E: compliance@smartfinancial.com.au

Generally, we will endeavour to respond or resolve your complaint as quickly as possible. If you are not satisfied with the outcome provided, or we have not responded within 30 days of receipt of your

complaint, you can refer your issue to the OAIC or the Australian Financial Complaints Authority (AFCA)

OAIC

GPO Box 5218,
Sydney NSW 2001
Email: enquiries@oaic.gov.au
Call: 1300 363 992

Australian Financial Complaints Authority

GPO Box 3 Melbourne VIC 3001
Email: info@afca.org.au
Call: 1800 931 678

Glossary

Australian Privacy Principles (APP's)

The Australian Privacy Principles are principles-based law. There are thirteen privacy principles that must be complied with.

Cookie

Means a small file that is placed on your device when you visit a website (including our Sites). In this Policy, a reference to a "Cookie" includes analogous technologies such as web beacons and clear GIFs.

Personal Information

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

Sensitive Information

Sensitive information is personal information that includes information or an opinion about an individual's: racial or ethnic origin; political opinions or associations; religious or philosophical beliefs or affiliations; trade union membership or associations; sexual orientation or practices; criminal record; health or genetic information; or some aspects of biometric information. Generally, sensitive information has a higher level of privacy protection than other personal information.

Site

Means any website operated, or maintained, by us or on our behalf.