Privacy Policy

Coastal Financial Services Pty Ltd Privacy Policy | Effective date: 11 November 2026

Our commitment to privacy

Coastal Financial Services Pty Ltd (we, us or our) respects your privacy and is committed to handling personal information responsibly. This policy explains how we collect, hold, use and disclose personal information when providing financial advice and related services.

We aim to comply with the Privacy Act 1988 (Cth), the Australian Privacy Principles and other privacy obligations that apply to our business.

Personal information we collect and why

Personal Information is information or an opinion that identifies an individual. The types of Personal Information we collect include, but are not limited to:

- Names
- Addresses
- Email addresses
- Phone numbers
- Financial information
- Investment details
- Tax File Numbers
- Any other information necessary to provide our services

Tax File Numbers are collected, used, stored and disclosed in accordance with the Privacy Act, the Tax File Number Rule 2015 and other applicable laws. We will only collect your TFN where authorised or required and will take additional security measures to protect it.

We collect your Personal Information primarily to:

- Provide tailored financial services to you
- Comply with legal and regulatory obligations
- Improve our services

We may also use your Personal Information for secondary purposes closely related to the primary purpose, in circumstances where you would reasonably expect such use or disclosure. You may unsubscribe from our mailing or marketing lists at any time by contacting us in writing.

How We Collect Personal Information

We collect Personal Information through various means, including:

- Face-to-face meetings
- Telephone calls
- Emails
- Our website
- Online forms
- From third-party service providers
- From publicly available sources

Where appropriate and possible, we will explain why we are collecting your information and how we plan to use it.

Sensitive Information

Sensitive Information is defined in the Privacy Act to include information or opinions about such things as an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trade union or other professional body, criminal record, or health information.

We will collect Sensitive Information only with your express consent unless required or authorised by law. Sensitive Information will be used by us only:

- For the primary purpose for which it was obtained
- For a secondary purpose that is directly related to the primary purpose
- With your consent
- Where required or authorised by law

Third Parties

Where reasonable and practicable, we will collect your Personal Information only from you. However, in some circumstances, we may receive information from third parties. In such cases, we will take reasonable steps to ensure that you are aware of the information provided to us by the third party.

Why we collect, use and disclose information

We may handle personal information to:

- verify identity and meet legal and regulatory obligations;
- assess your circumstances, objectives and needs;
- prepare, provide, implement and review financial advice;
- arrange or administer financial products and services;
- communicate with you and manage our relationship;

- process payments and maintain business records;
- manage risk, security, complaints, disputes and professional obligations;
- improve our services and conduct analytics; and
- send marketing communications where permitted, subject to your right to opt out.

If you do not provide requested information, we may be unable to:

- provide financial advice;
- verify your identity;
- establish or administer products;
- comply with legal obligations; or
- continue providing services.

Who we may disclose information to

Where reasonably necessary, authorised or required by law, we may disclose personal information to:

- our Australian Financial Services Licensee, authorised representatives, employees and related entities;
- financial product providers, platforms, insurers, superannuation funds and service providers;
- professional advisers, auditors, compliance consultants and dispute-resolution bodies;
- technology, cloud, data-storage, document, communication and security providers;
- identity-verification, fraud-prevention and credit-reporting organisations where applicable;
- government agencies, regulators, courts and law-enforcement bodies; and
- a prospective purchaser or successor in connection with a business transaction, subject to appropriate safeguards.

Overseas disclosure and storage

We may disclose Personal Information to overseas recipients, including cloud hosting, software and outsourcing service providers. These recipients are currently located in the Philippines.

A current list of overseas jurisdictions in which our key service providers are located is available upon request.

Before disclosing Personal Information overseas, we take reasonable steps to ensure the recipient does not breach the Australian Privacy Principles, including through contractual privacy, confidentiality and security obligations. We remain accountable for the handling of that information in accordance with the Privacy Act 1988 (Cth).

Security and retention

We use reasonable administrative, technical and physical safeguards designed to protect personal information from misuse, interference, loss and unauthorised access, modification or disclosure.

Our information security framework includes controls such as:

- multi-factor authentication (MFA);
- role-based access controls;
- encryption of data in transit and at rest where appropriate;
- cybersecurity awareness training;
- vulnerability and patch management processes;
- data backup and recovery procedures;
- incident response and breach escalation processes; and
- regular staff training on privacy obligations

We may store personal information electronically using secure cloud-based systems, including document management, customer relationship management, communication and collaboration platforms.

These systems may include providers such as Microsoft 365, SharePoint, Teams, cloud backup services and other business applications used to provide financial services. Personal Information may be stored or processed in Australia and other countries where our technology providers operate data centres or support services.

We take reasonable steps to ensure service providers implement appropriate privacy and security safeguards, including encryption, access controls, monitoring and data backup procedures.

We retain personal information for as long as needed for our services and legal, regulatory, insurance and recordkeeping obligations. When your Personal Information is no longer needed for the purpose for which it was obtained, we will take reasonable steps to destroy or permanently de-identify it.

We retain personal information for the period required by law and our legitimate business, regulatory and insurance obligations. In many cases, financial advice records will be retained for at least seven years and may be retained for longer where required or permitted.

You may also request deletion of your personal information by contacting us. Deletion may not always be possible if we are legally obligated to retain certain data.

We use third-party technology and service providers to support our operations, including:

- client relationship management systems;
- financial planning software;
- document management systems;
- electronic signature platforms;
- cloud hosting providers;
- cyber security services; and
- communication and collaboration platforms.

These providers may access or process personal information on our behalf solely for authorised purposes and subject to appropriate contractual obligations.

Artificial Intelligence (AI), Automated Processing and Computer-Based Decision Making

We may use artificial intelligence (AI), computer programs and other automated technologies to assist us in providing services, improving operational efficiency, managing risk, detecting and preventing fraud, maintaining cybersecurity, meeting legal and regulatory obligations, conducting compliance monitoring, verifying identity, onboarding clients and supporting our day-to-day business operations.

Where these technologies process personal information, the kinds of personal information used may include identity and contact information, financial information, transaction information, verification and authentication information, client instructions, communications, and device or system information relevant to the service being provided.

Some of our systems may use automated processing or computer-based decision making to assist with activities such as identity verification, fraud detection, cybersecurity monitoring, transaction monitoring, risk assessment, compliance management, regulatory reporting and other operational or administrative functions. These systems may assist our staff in making decisions or taking action but do not replace human oversight where professional judgement is required.

We do not use AI or automated decision-making systems as the sole basis for providing personal financial advice, determining the suitability of financial strategies, or making recommendations to clients. Our authorised representatives and staff remain responsible for the advice, services and decisions we provide.

Where we use computer programs, AI systems or automated processing in a manner that is reasonably likely to significantly affect an individual's rights or interests, we will take reasonable steps to ensure appropriate governance, oversight and compliance with applicable privacy laws. Information about:

- the kinds of personal information used in those processes;
- the kinds of decisions made or substantially assisted by automated processing; and
- how those processes operate, may be obtained by contacting us using the details set out in this Privacy Policy.

We take reasonable steps to protect personal information used in AI and automated systems through appropriate privacy, security and confidentiality controls. We do not knowingly permit client personal information to be used to train publicly available AI systems unless we have notified you and, where required by law, obtained your consent.

Some AI-enabled, cloud-based or technology service providers may process or store personal information outside Australia. Information about overseas disclosures and storage arrangements is set out in the "Overseas Disclosure and Storage" section of this Privacy Policy.

Anonymity

Where lawful and practicable, you may deal with us anonymously or using a pseudonym. However, due to the nature of financial advice services and our legal obligations, including AML/CTF and identification requirements, we will generally need to collect information that identifies you before we can provide advice or services.

Data breaches

We maintain processes for responding to suspected data breaches. Where required, we will notify affected individuals and the Office of the Australian Information Commissioner.

A data breach may occur if your Personal Information is lost or subjected to unauthorised access, modification, disclosure or other misuse or interference, and it is generally notifiable if there is a risk of ‘serious harm’ (for example, financial or reputational harm) to you due to the breach. This obligation extends to breaches that occur within Australia, and overseas.

We will also report any privacy breach as required under any other applicable laws.

Access and correction

You may request access to personal information we hold about you or ask us to correct information that is inaccurate, out of date, incomplete, irrelevant or misleading. Contact our Privacy Officer using the details below. We will respond within a reasonable period and explain any lawful reason for refusing a request. We may charge a reasonable fee for providing access, but not for making a request.

Direct marketing

We may send information about services that may be relevant to you where permitted by law. You may opt out at any time by using an unsubscribe facility or contacting us. We will action opt-out requests within the period required by law.

Digital services, cookies and third-party links

Our websites or digital services may use cookies and similar technologies to operate, secure and improve those services and understand usage. You may adjust browser settings to restrict cookies, although some features may not function properly. Third-party websites are governed by their own privacy practices.

We may use analytics and advertising technologies to understand website usage, improve our services and measure the effectiveness of marketing campaigns.

Complaints and Enquiries

If you would like further information about how we handle your personal information, please send us an email to enquiries@mkfinancialplanning.com.au.

If you wish to make a complaint in relation to privacy, including a breach of the Australian Privacy Principles, you can let us know by putting your concerns in writing or call us.

Business: Coastal Financial Services Pty Ltd
Address: PO Box 750, Coolangatta QLD 4225
Email: enquiries@mkfinancialplanning.com.au
Phone: 07 55363936

We aim to acknowledge complaints within 5 business days and respond within 30 days, unless a longer period is permitted by law.

If you are not satisfied with our response, you may contact the Office of the Australian Information Commissioner (OAIC) at:

GPO Box 5218, Sydney NSW 2001

Email: enquiries@oaic.gov.au
Phone: 1300 363 992

Policy Updates

We may update this policy from time to time. The current version will show its effective date and will be available at www.mkfinancialplanning.com.au.

Document Control

Document Information	Details
Document Name	Privacy Policy
Owner	Compliance
Version	1.0
Effective Date	11 November 2026
Next Review Date	11 November 2027