SUMMIT THROUGH DISCIPLINE

CENTRAL ACCORD

BRINGING YOUR WEALTH INTO ACCORD

Privacy Policy

Privacy

CENTRAL ACCORD PTY LTD

10-20 Gwynne Street, Cremorne VIC 3121 | +61 3 8618 6943 | support@centralaccord.com.au

Central Accord Pty Ltd

ACN 068 486 126 · ABN 93 068 486 126 · AFSL 226405

www.centralaccord.com.au · +61 3 8618 6943 · 1300 753 199

10-20 Gwynne Street, Cremorne VIC 3121

Privacy

Privacy at a glance

This section summarises how Central Accord Pty Ltd handles personal information. It is a guide to the key information only and should be read together with the full Privacy Policy that follows.

Our commitment	**We collect only what we need, use it for clear and lawful purposes, protect it carefully, and support your rights to access, correct and complain about how personal information is handled.**
What we collect	Identity and contact details, financial and employment information, product and service information, communications, digital information and sensitive information where relevant and permitted by law.
Why we collect it	To provide advice and related services, understand your needs, verify identity, administer products, meet legal obligations, improve our services and manage our relationship with you.
Who we may share it with	Authorised representatives, product providers, platforms, professional advisers, technology and administration providers, regulators and other parties where required or authorised.
Digital services and cookies	Our website and digital services may collect device, usage, analytics and cookie information to operate services, improve experience and keep systems secure.
Your rights	You can request access to, or correction of, personal information we hold about you. You can also make a privacy complaint at no cost.
Need help?	Contact the Privacy Officer using the details at the end of this Policy. We can also support accessibility or communication needs where reasonably possible.

Full Privacy Policy

This Privacy Policy explains how personal information is collected, used, disclosed, stored and protected, and how privacy rights can be exercised.

1. Our commitment

At Central Accord Pty Ltd, we recognise that the privacy and security of personal information are important to the trust you place in us.

We are committed to protecting personal information and handling it in a lawful, fair, transparent and secure manner.

This Privacy Policy explains how we collect, use, disclose, store, protect and manage personal information in accordance with the Privacy Act 1988 (Cth), the Australian Privacy Principles and other applicable privacy and financial services obligations.

2. What is personal information?

Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable.

Examples include your name, address, contact details, date of birth, identification information and financial information.

Sensitive information is a special category of personal information. It may include health information, medical information, racial or ethnic origin, professional or trade association membership, religious beliefs or other information protected under privacy law.

3. When you can deal with us without identifying yourself

You may deal with us anonymously or by using a pseudonym where it is lawful and practicable to do so.

In many cases, we will need to identify you before we can provide financial advice or related services. This may be required so we can verify your identity, meet anti-money laundering and counter-terrorism financing obligations, satisfy taxation or superannuation requirements, assess your circumstances, or comply with financial services record-keeping obligations.

Where we cannot provide a service without identifying you, we will explain this where practicable.

4. Collection of personal information

We collect personal information that is reasonably necessary for our services, our relationship with you and our legal and regulatory obligations.

The personal information we collect may include:

- identity and contact details, including name, date of birth, address, email and phone number;
- financial, employment, income, asset, liability, expense, insurance, superannuation and tax information;
- information about your objectives, needs, circumstances, risk profile and financial products;
- government-related identifiers where required or authorised by law, such as Tax File Numbers, driver licence numbers or passport details;
- communications, meeting notes, application forms, consent records and service history;
- information about family members, beneficiaries, dependants, trustees, attorneys or other related parties where relevant to the services requested;
- health, medical or other sensitive information where relevant to insurance, financial advice or another service and where permitted by law; and
- website and digital information such as IP address, device information, browser settings, pages visited, time of access and cookies or similar technologies.

We generally collect personal information directly from you. We may also collect information from third parties where you have authorised this, where it is reasonably expected, or where permitted or required by law.

These third parties may include financial advisers, accountants, lawyers, employers, product issuers, platform providers, insurers, medical or health professionals, government agencies, identity verification providers, publicly available sources and service providers engaged to assist with our services or operations.

5. Government identifiers

We only collect Tax File Numbers and other government-related identifiers where required or authorised by law.

This may include Tax File Numbers, driver licence details, passport details or other identifiers where they are reasonably necessary for identity verification, taxation, superannuation, insurance, anti-money laundering or other legal and regulatory obligations.

Government identifiers are handled securely and are not used as general client identifiers.

6. How we use personal information

We may use personal information for purposes including:

- providing financial advice and related services;
- understanding your needs, objectives and circumstances;
- preparing, reviewing and implementing advice documents, applications and service arrangements;
- verifying your identity and satisfying anti-money laundering, counter-terrorism financing, taxation, financial services and other legal obligations;
- administering products, platforms, accounts, payments, fees, consent arrangements and ongoing services;
- communicating with you and your authorised representatives;
- responding to enquiries, access requests, correction requests, complaints and disputes;
- maintaining records, audit trails, quality assurance, compliance monitoring and supervision;
- protecting information security, detecting fraud and managing cyber or operational risks;
- managing our business operations, reporting, training, analytics, insurance, legal and professional obligations; and
- providing service updates, educational content, invitations or information that may be relevant to you, where permitted by law.

7. Disclosure of personal information

We may disclose personal information where required or authorised by law, where you have consented, where you would reasonably expect us to do so, or where disclosure is reasonably necessary for our services or business operations.

Recipients may include:

- your authorised representatives, including advisers, accountants, lawyers, trustees, attorneys or nominated contacts;
- financial product issuers, platform providers, insurers, superannuation funds, investment managers and other product or service providers;
- financial planning, CRM, advice, portfolio administration, document management, digital signature and client portal providers;
- paraplanning, administration, mailing, printing, archiving and business support providers;
- technology, cloud hosting, cybersecurity, identity verification, analytics and IT support providers;
- payment processors, banks and other payment system participants;
- auditors, compliance consultants, insurers, legal advisers, professional advisers and external dispute resolution bodies;
- regulators, government agencies, courts, tribunals, law enforcement agencies and professional or industry bodies; and
- other parties where required or authorised by law.

We require representatives and service providers who handle personal information on our behalf to comply with appropriate confidentiality, privacy and information security obligations.

8. Direct marketing and communications

We may use your personal information to provide service updates, educational content, invitations, product information, news or marketing communications that may be relevant to you, where permitted by law.

You may opt out at any time by contacting us or using the unsubscribe facility in the relevant communication.

We will not sell personal information to third parties.

9. Overseas disclosure

Some service providers may be located outside Australia or may store, process or access information using infrastructure located outside Australia.

The countries or regions where overseas recipients are likely to be located may vary depending on the technology, cloud hosting, cybersecurity, document preparation, administration, analytics, professional services and business support providers used from time to time. Central Accord maintains an internal overseas disclosure register to record these locations and can provide further information where reasonably practicable.

Where personal information is disclosed overseas, we take reasonable steps to ensure the recipient handles the information in a manner consistent with Australian privacy obligations, unless an exception applies under law.

10. Data security and protection

We take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, unauthorised modification and unauthorised disclosure.

Our security measures may include:

- privacy, cybersecurity and confidentiality training;
- access controls, role-based permissions, strong password controls and multi-factor authentication;
- secure cloud, CRM, financial planning, document management and record-keeping systems;
- encryption where appropriate;
- cybersecurity monitoring, vendor due diligence and third-party security reviews;
- backup, recovery and business continuity controls; and
- incident response, cyber incident and data breach management procedures.

No method of electronic transmission or storage is completely secure. We maintain layered controls and review them as our services, risks and technology environment evolve.

11. Retention and destruction

We retain personal information for as long as required for our services, legal obligations, regulatory requirements, dispute management, insurance, audit, compliance and business purposes. This may include retaining advice records for at least seven years and retaining customer identification records for the statutory period after the relevant relationship ends.

Where personal information is no longer required, we take reasonable steps to de-identify it or securely destroy it, subject to legal, regulatory, archival, dispute or operational requirements.

12. Website, cookies and digital information

When you use our websites, portals, online forms, social media pages or digital services, we may collect certain information automatically, including:

- IP address, device identifiers and general location information;
- browser type, device type, operating system and settings;
- pages visited, links selected, forms started or submitted and usage activity;
- time, date and duration of access;
- referring websites, campaign information and interaction data; and
- cookies, pixels, log files, web beacons and similar technologies.

We use this information to operate our website, improve user experience, monitor performance, support security, analyse trends, maintain records, provide relevant content and improve our services.

You can usually manage or disable cookies through your browser settings, but this may affect some website functionality.

13. Third-party platforms and website redirects

Our website may provide general information, disclosure documents, consent pathways, login links, portal links or redirect pathways to third-party platforms. These platforms may include product administration platforms, product issuer portals, client portals, CRM systems, advice systems, document management systems, digital signing tools or other service providers.

Where our website redirects you to a third-party platform or service provider, you are entering a separate platform operated by that provider. That provider is responsible for its own platform operations, security controls, platform disclosures and privacy practices.

We remain responsible for our own website content, privacy notices, consent processes, client relationship, advice obligations and any personal information we collect or control.

14. Access and correction

You may request access to personal information we hold about you. You may also request correction if you believe information is inaccurate, incomplete, out of date, irrelevant or misleading.

Requests should be directed to your adviser or to the Privacy Officer using the contact details at the end of this policy.

We aim to respond to access and correction requests within 30 days, subject to the nature and complexity of the request. A reasonable administrative fee may apply for providing access to certain records. We will not charge a fee for making a correction request.

In some circumstances, we may refuse access or correction where permitted or required by law. If this occurs, we will provide reasons where required and explain available complaint options.

15. Privacy complaints

If you are concerned about how we have handled your personal information, you may lodge a privacy complaint with us.

Complaints can be made to the Privacy Officer using the contact details at the end of this policy.

We will acknowledge receipt of your complaint within 24 hours, or as soon as reasonably practicable. We aim to investigate and respond within 30 days.

If you are not satisfied with our response, or if we do not respond within a reasonable period, you may contact:

- Office of the Australian Information Commissioner - for privacy-related matters. Website: www.oaic.gov.au.
- Australian Financial Complaints Authority - where the matter relates to financial services and falls within AFCA's jurisdiction. Website: www.afca.org.au.

16. Notifiable data breaches

We maintain procedures for assessing and responding to suspected data breaches.

Where we reasonably believe an eligible data breach has occurred, we will take steps required under the Notifiable Data Breaches scheme, including notifying affected individuals and the Office of the Australian Information Commissioner where required by law.

We may also take steps to contain, investigate, remediate and reduce the risk of recurrence.

17. Changes to this Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in law, regulatory guidance, business practices, services, technology or information handling arrangements.

The latest version will be available on our website. We encourage you to review it periodically.

18. Contact us

For privacy-related enquiries, access requests, correction requests or complaints, please contact:

Privacy Officer

Central Accord Pty Ltd

10-20 Gwynne Street, Cremorne VIC 3121

Telephone: +61 3 8618 6943

Email: privacy@centralaccord.com.au

Website: www.centralaccord.com.au

Please clearly state that your request or complaint is privacy-related so it can be directed to the Privacy Officer.

Version control

Version	**1.3**
Effective date	12 February 2026
Owner	Head of Risk and Compliance
Issued by	Central Accord Pty Ltd
Summary of changes	New Central Accord Privacy Policy