



Cashflow Financial

Privacy Policy

Last updated: 29 September 2026

Version 2.29.9.2026

At **Cashflow Financial**, we are committed to protecting your privacy and handling your personal information responsibly. As a trusted provider of accounting and financial planning services, we understand the sensitive nature of the information you entrust to us.

This Privacy Policy explains how we collect, use, store, disclose, and protect your personal information in accordance with the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs).

Contents

- Our Commitment to Privacy
- Information We Collect
- How We Use Your Information
- Security and Protection of Your Information
- Automated Decision-Making
- Disclosure of Your Information
- Cross-Border Disclosure
- Data Breaches and Notification
- Cookies and Website Technology
- Your Rights and Choices
- Children's Privacy
- Updates to This Policy
- How to Contact Us

1. Our Commitment to Privacy

Cashflow Financial is bound by the Privacy Act 1988 (Cth) and adheres to the 13 Australian Privacy Principles. We implement comprehensive practices, procedures, and systems to ensure compliance with our privacy obligations and to manage personal information in an open and transparent manner.

As a professional accounting and financial planning practice, we also comply with:

- Tax Practitioners Board (TPB) Code of Professional Conduct
- Financial Planners and Advisers Code of Ethics 2019
- Australian Securities and Investments Commission (ASIC) regulatory requirements
- Professional standards and ethical obligations applicable to our industry

2. Information We Collect

2.1 Types of Personal Information

In providing our accounting and financial planning services, we may collect and hold various types of personal information, including:

Identity and Contact Information:

- Full name, date of birth, and gender
- Contact details (address, email, phone numbers)
- Identification documents (driver's licence, passport details)
- Tax File Number (TFN) and Australian Business Number (ABN)

Financial Information:

- Income, assets, liabilities, and financial position
- Bank account details and payment information
- Investment portfolios and superannuation details

- Credit history and credit reporting information
- Tax records and financial statements

Business Information:

- Company name, ACN/ABN, and business structure
- Director and shareholder information
- Business financial records and performance data

Personal Circumstances:

- Marital status and family composition
- Employment details and occupation
- Financial goals and risk tolerance
- Estate planning information

Website and Digital Information:

- IP address and device information
- Browser type and operating system
- Website usage data and navigation patterns
- Form submissions and enquiry details

2.2 How We Collect Information

We collect personal information directly from you through:

- Initial consultation meetings and ongoing client interactions
- Client engagement forms and service agreements
- Documents you provide for tax return preparation, financial planning, or advisory services
- Email, telephone, and written correspondence
- Our website, including contact forms and online booking systems
- Our client portal and secure file sharing systems
- Our website chat assistant, including any details you type into a conversation or the call-back request form
- Our Cashflow Financial employees may record client interactions for note-taking purposes. If you do not consent to being recorded, please let the employee know at the start of the interaction.

We may also collect information from third parties, including:

- The Australian Taxation Office (ATO)
- Financial institutions and product providers
- Credit reporting agencies
- Your authorised representatives or agents
- Professional advisers (with your consent)

We will only collect personal information that is reasonably necessary for our functions and activities. Where practicable, we will collect information directly from you and inform you of the purposes for collection at the time.

2.3 Sensitive Information

We do not generally collect sensitive information (such as health information, racial or ethnic origin, political opinions, or criminal records) unless it is reasonably necessary for our services and you have consented, or we are required or authorized by law to do so. In limited circumstances, we may collect health information relevant to insurance or estate planning advice with your explicit consent.

3. How We Use Your Information

3.1 Primary Purposes

We use your personal information for the primary purpose for which it was collected, including to:

- Prepare and lodge tax returns and Business Activity Statements (BAS)
- Provide financial planning advice and recommendations
- Establish and administer Self-Managed Super Funds (SMSFs)
- Provide business advisory and compliance services
- Prepare financial statements and reports
- Communicate with you about your services and account
- Process payments and manage billing

- Comply with legal and regulatory obligations
- Maintain professional indemnity insurance

3.2 Secondary Purposes

We may also use your information for related secondary purposes where you would reasonably expect such use, or where permitted by the APPs, including:

- Internal administration and record-keeping
- Quality assurance and staff training
- Business systems development and improvement
- Risk management and fraud prevention
- Statistical analysis and research (using de-identified data)

3.3 Marketing Communications

We may use your contact information to send you newsletters, updates, and information about our services that we believe may be of interest to you. Marketing communications will only be sent if you have:

- Requested or subscribed to receive such communications; or
- Provided your consent; or
- Where permitted by applicable law for existing client relationships

You can opt out of marketing communications at any time by using the unsubscribe link in our emails, contacting us directly, or updating your preferences in our client portal. Your request will be actioned immediately, and this will not affect your ability to receive service-related communications.

4. Security and Protection of Your Information

4.1 Our Security Commitment

We are committed to protecting your personal information from misuse, interference, loss, unauthorised access, modification, or disclosure. We implement technical and organisational measures appropriate to the sensitivity and nature of the information we hold.

4.2 Security Measures

Our security measures include:

- Encryption of data in transit and at rest
- Secure access controls and multi-factor authentication
- Regular security assessments and penetration testing
- Firewall protection and intrusion detection systems
- Secure server infrastructure and data storage facilities
- Physical security controls and access restrictions
- Secure destruction of physical records when no longer required
- Comprehensive staff training on privacy and information security
- Confidentiality agreements with all staff and contractors
- Regular backups and disaster recovery procedures

4.3 Data Storage Infrastructure

We use a combination of infrastructure solutions to store and manage your personal information securely:

- **Secure server infrastructure:** We maintain secure server infrastructure, which may include on-premise servers, co-location facilities, or cloud-based infrastructure, all configured to Australian data protection standards
- **Cloud services:** We use enterprise-grade cloud services, primarily from Microsoft (including Microsoft 365, Azure, and related services), configured for Australian data residency where available

We regularly review our infrastructure to ensure it meets evolving security standards and business continuity requirements. Our infrastructure choices are guided by the principles of security, reliability, and compliance with Australian privacy laws.

4.4 Data Retention and Destruction

We retain your personal information for as long as necessary to provide our services and as required by law. Australian tax and accounting records must generally be retained for a minimum of seven years. Financial planning records are retained in accordance with ASIC requirements.

When personal information is no longer required, we will take reasonable steps to destroy or de-identify it in a secure manner, unless we are required by law to retain it.

4.5 Credit Card Information

Credit card information used for payment processing is encrypted before transmission using industry-standard SSL/TLS protocols. We do not store complete credit card details on our servers. Payment processing is handled by PCI-DSS compliant third-party payment processors.

5. Automated Decision-Making

We may use computer programs and automated systems that process personal information to assist in making decisions or performing tasks related to our services.

5.1 Types of Automated Processing

The types of automated decision-making we may use include:

- **Tax calculation software:** We use professional tax preparation software that processes your financial information to calculate tax liabilities, deductions, and entitlements. While these systems automate calculations, all tax returns are reviewed and verified by qualified tax practitioners before lodgement.
- **Financial planning software:** Our financial planning tools use algorithms to model investment scenarios, retirement projections, and risk assessments based on your personal and financial circumstances. These automated analyses support our advisers in developing recommendations, but final advice is always provided by qualified financial planners who review and interpret the results.
- **Document management systems:** We use automated systems to categorise, index, and manage client documents based on document type, date, and other metadata.
- **Accounting and bookkeeping software:** Automated processing of transactions, bank reconciliations, and financial reporting using platforms such as Xero and MYOB.

5.2 Personal Information Used

The kinds of personal information that may be processed by automated systems include:

- Financial data (income, expenses, assets, liabilities)
- Investment and superannuation information
- Tax File Numbers and identification details
- Personal circumstances (age, employment, family situation)
- Risk tolerance and financial goals

5.3 Human Oversight and Review

It is important to note that:

- No significant decisions affecting your rights or interests are made solely by automated systems without human review
- All tax returns, financial advice, and significant recommendations are reviewed and approved by qualified professionals
- You always have the right to discuss any automated outputs with your adviser
- You can request human intervention in any automated process affecting your services

If you have questions about how automated systems are used in relation to your information, please contact our Privacy Officer using the details at the end of this policy.

6. Disclosure of Your Information

6.1 When We Disclose Information

We do not sell, trade, or rent your personal information to third parties. We may disclose your personal information to third parties only in the following circumstances:

- **With your consent:** Where you have provided explicit or implied consent for the disclosure
- **Service provision:** To deliver the services you have requested
- **Legal requirements:** Where required or authorised by law
- **Legal protection:** To protect our legal rights, property, or safety, or that of others
- **Business transitions:** In the event of a merger, sale, or transfer of assets (under confidentiality agreements)

6.2 Third Parties We May Disclose To

We may disclose your personal information to the following types of third parties:

- **Government agencies:** Australian Taxation Office (ATO), Australian Securities and Investments Commission (ASIC), and other regulatory bodies as required by law
- **Financial institutions:** Banks, investment platforms, superannuation funds, and insurance providers to facilitate financial transactions and implement recommendations
- **Professional advisers:** Lawyers, auditors, and other professional advisers (with your consent)
- **Technology service providers:** Cloud storage providers, IT support, software vendors, hosting providers, and data backup services
- **Payment processors:** Third-party payment gateway providers for processing client payments
- **Professional indemnity insurers:** For insurance coverage and claims management
- **Related entities:** Other entities within the Cashflow Financial group for operational purposes

We require all third-party service providers to comply with the APPs or equivalent privacy standards and to only use your personal information for the specific purpose for which it was shared. Our contracts with third parties include strict confidentiality and data protection obligations.

7. Cross-Border Disclosure of Personal Information

7.1 Overseas Access to Information

In the course of providing our services, your personal information may be accessed by or disclosed to overseas recipients. Under the Privacy Act, we are responsible for ensuring appropriate privacy protections are in place for any cross-border access to or disclosure of personal information.

7.2 Overseas-Based Staff and Service Providers

We may employ staff members or engage service providers located overseas who access personal information as part of their duties in providing accounting, administrative, or technical support services. This access is considered a cross-border disclosure under the Privacy Act.

Currently, we have offshore staff in the Philippines employed by PBIS, who may access client information stored on our servers. Our overseas staff:

- Are bound by the same confidentiality obligations as our Australian staff
- Access information only as necessary to perform their assigned duties
- Connect to our systems through secure, encrypted connections
- Receive regular training on privacy and information security requirements
- Are subject to the data protection laws of their country, including the Philippines Data Privacy Act of 2012

We maintain effective control over the personal information accessed by our overseas staff and service providers, and remain accountable under Australian privacy law for their handling of this information.

7.3 Cloud Services and International Data Processing

We use cloud-based software and services from enterprise technology providers. While we configure these services for Australian data residency where available, some data processing may occur internationally as part of the providers' global infrastructure operations.

AI service providers: Our website chat assistant is provided through Anthropic, a United States-based AI provider. Conversations entered into the chat assistant are processed in the United States to generate a response.

Our primary cloud service provider is Microsoft (including Microsoft 365, Azure, and related services). Your personal information may be processed or stored in the following locations through our use of cloud services and technology infrastructure:

- **Australia:** We prioritise Australian data residency for cloud services where available and configure our systems accordingly

- **United States:** Some cloud services and features may process data in US data centres as part of global infrastructure
- **European Union:** Data may be processed in EU data centres where cloud providers operate regional infrastructure
- **Asia-Pacific region:** Including Singapore, Japan, and other countries where our cloud and technology providers operate data centres
- **Other countries:** Where our technology service providers operate infrastructure or provide services as part of their global networks

The specific countries where your data may be processed can vary as cloud providers expand or modify their global infrastructure. For current information about Microsoft's data centre locations and data residency practices, visit the Microsoft Trust Center at <https://www.microsoft.com/en-us/trust-center>.

7.4 Safeguards for Cross-Border Disclosure

When we disclose personal information to overseas recipients or allow overseas access to personal information, we:

- Take reasonable steps to ensure the recipient complies with the Australian Privacy Principles
- Prioritise recipients in countries or schemes that have been approved by the Minister as providing substantially similar privacy protections to Australia
- Include contractual privacy obligations in our agreements with overseas service providers
- Implement technical security measures such as encryption and secure access controls
- Conduct due diligence on the privacy practices and security capabilities of overseas recipients
- Maintain oversight and audit rights over overseas processing activities
- Provide comprehensive training to all staff, including overseas staff, on Australian privacy requirements
- Select service providers with robust privacy and security certifications and frameworks

7.5 Your Rights Regarding Cross-Border Disclosure

We remain accountable under Australian law for how your personal information is handled by overseas recipients. This means:

- You can make complaints to us about the handling of your information by overseas recipients
- We are responsible for investigating and addressing such complaints
- The Office of the Australian Information Commissioner can investigate breaches involving overseas recipients
- Your privacy rights under the APPs continue to apply

8. Data Breaches and Notification

8.1 Our Data Breach Response

We have comprehensive incident response procedures in place to identify, contain, and respond to potential data breaches. Our procedures include immediate investigation, assessment of the breach, and implementation of remedial actions to prevent harm.

8.2 Notifiable Data Breach Obligations

Under the Notifiable Data Breaches (NDB) scheme, we are required to notify you and the Office of the Australian Information Commissioner (OAIC) if:

- There is unauthorised access to, unauthorised disclosure of, or loss of your personal information
- This is likely to result in serious harm to you
- We have not been able to prevent the likely risk of serious harm through remedial action

8.3 Assessment and Notification Process

If we suspect a data breach may have occurred, we will:

- Conduct a prompt assessment (generally within 30 days) to determine if it is an eligible data breach

- Take immediate action to contain the breach and prevent further unauthorised access
- Implement remedial measures to reduce the risk of serious harm
- Where required, notify affected individuals and the OAIC as soon as practicable

8.4 What We Will Tell You

If we need to notify you of an eligible data breach, we will provide:

- A description of the data breach
- The kinds of personal information involved
- The steps we have taken to respond to the breach
- Recommendations on steps you should take to reduce the risk of harm (such as changing passwords, monitoring accounts, or being alert to identity fraud)

8.5 How We Will Notify You

Notification may be provided by:

- Email to your registered email address
- Telephone call
- Written letter to your postal address
- If we cannot contact everyone affected, we will publish a notification on our website and promote it through appropriate channels

8.6 Ransomware and Cyber Extortion Reporting

In accordance with the Cyber Security Act 2024, we are also required to report any ransomware or cyber extortion payments to the Australian Cyber Security Centre within 72 hours. This reporting is in addition to our obligations under the NDB scheme.

9. Cookies and Website Technology

9.1 What Are Cookies

A cookie is a small text file placed on your device by our website that collects information about your web browsing behaviour. Cookies help us provide you with a better website experience by remembering your preferences and understanding how you use our site. Cookies do not access other information stored on your device or any personal data such as your name, address, email, or telephone number.

9.2 How We Use Cookies

Our website uses cookies for:

- **Website analytics:** To analyse website traffic, understand user behaviour, and improve our website performance using services such as Google Analytics
- **Essential functionality:** To enable core website features such as secure login to our client portal and maintaining your session
- **User preferences:** To remember your preferences and settings
- **Social media integration:** To provide social media sharing and interaction functionality (Facebook, LinkedIn, Twitter)

9.3 Third-Party Cookies and Pixels

We may use cookies and pixels from third-party services such as Google Ads and Facebook Adverts to serve relevant advertisements to website visitors. These ads may appear on our website or on other websites you visit. These third parties may collect information about your online activities over time and across different websites.

9.4 Managing Cookies

Most web browsers automatically accept cookies, but you can modify your browser settings to decline cookies if you prefer. Please note that disabling cookies may prevent you from taking full advantage of our website and may affect the functionality of certain features, such as:

- Accessing our secure client portal
- Using the online booking system
- Remembering your preferences

For more information about managing cookies, please visit your browser's help pages or www.aboutcookies.org.

9.5 Website Chat Assistant

Our website includes an automated chat assistant that can answer general questions about our services. The assistant is powered by artificial intelligence (AI) and does not provide personal financial, tax or legal advice.

When you use the chat assistant:

- The text of your conversation is sent to our AI service provider, Anthropic, to generate a reply. Anthropic is based in the United States, and your conversation may be processed outside Australia.
- We do not use the chat assistant to make decisions about you, and its responses are not reviewed by a person before they appear.
- If you ask to be contacted and complete the call-back request form, the details you provide (such as your name, phone number, email address and the service you're interested in) are sent to our team so we can respond to you.

Please do not enter your Tax File Number, bank account details, passwords, identification documents or other sensitive information into the chat assistant. If you need to share this information, please contact our office directly.

10. Your Rights and Choices

You have several rights regarding your personal information under the Privacy Act:

10.1 Right to Access

You have the right to request access to the personal information we hold about you. To request access, please contact our office in writing using the details at the end of this policy. We will respond to your request within 30 days and provide access in the format you request where reasonable and practicable. In some circumstances, we may charge a reasonable fee for providing access, which we will advise you of before proceeding.

10.2 Right to Correction

You have the right to request correction of personal information we hold about you if you believe it is inaccurate, out-of-date, incomplete, irrelevant, or misleading. We will take reasonable steps to correct your information within 30 days of your request. You can make corrections by:

- Contacting us directly by email, phone, or in writing
- Speaking with your adviser, accountant, or one of our staff members

If we refuse to correct your information, we will provide you with written reasons for our decision and inform you of your right to make a complaint.

10.3 Right to Complain

If you believe we have breached the Privacy Act or the Australian Privacy Principles, you have the right to make a complaint. To lodge a complaint:

- Contact our Privacy Officer using the details at the end of this policy
- Provide details of your complaint in writing
- Include any supporting information or documentation

We will acknowledge receipt of your complaint within 7 days and will investigate and respond within 30 days. If you are not satisfied with our response, you have the right to lodge a complaint with the Office of the Australian Information Commissioner (OAIC) at www.oaic.gov.au or by calling 1300 363 992.

10.4 Right to Opt-Out

You have the right to opt-out of:

- **Marketing communications:** Unsubscribe using the link in any marketing email, or contact us directly
- **Cookies:** Adjust your browser settings as described in Section 9.4

10.5 Limits on Access and Correction

In some circumstances, we may not be able to provide access to or correct your personal information. This includes where:

- Providing access would pose a serious threat to life, health, or safety

- Providing access would have an unreasonable impact on the privacy of others
- The request is frivolous or vexatious
- The information relates to existing or anticipated legal proceedings
- Providing access would reveal commercially sensitive information
- Providing access would be unlawful or prejudice enforcement activities

If we deny your request for access or correction, we will provide written reasons for our decision and inform you of your right to make a complaint to us or the OAIC.

11. Children's Privacy

Our services are not directed to individuals under 18 years of age, and we do not knowingly collect personal information from children under 18 without parental or guardian consent.

We may collect personal information about minors in the following circumstances:

- When providing family taxation services (with parental consent)
- For estate planning or trust establishment purposes
- When required for compliance with legal or regulatory obligations

If we become aware that we have collected personal information from a child under 18 without appropriate consent, we will delete that information as quickly as possible. If you are a parent or guardian and believe your child has provided us with personal information without your consent, please contact us immediately.

We are monitoring the development of the Children's Online Privacy Code being created by the Office of the Australian Information Commissioner and will update our practices and this policy as required when the Code comes into effect.

12. Updates to This Privacy Policy

We review and update this Privacy Policy regularly to ensure it remains current with our practices and complies with applicable privacy laws. The "Last updated" date at the beginning of this policy indicates when it was last revised.

If we make material changes to this policy that significantly affect how we handle your personal information, we will notify you by:

- Posting a prominent notice on our website
- Sending you an email notification (if we have your email address)
- Including a notice with your next service communication

We encourage you to review this Privacy Policy periodically to stay informed about how we protect your information. Your continued use of our services after any changes to this policy will constitute your acknowledgment of the changes and consent to the updated policy.

13. How to Contact Us

If you have any questions, concerns, or complaints about this Privacy Policy or how we handle your personal information, please contact us:

Cashflow Financial

Postal Address: Unit 306, Level 3/3-5 Stapleton Ave, Sutherland NSW 2232

Office Address: Unit 306, Level 3/3-5 Stapleton Ave, Sutherland NSW 2232

Phone: (02) [4258 3668](tel:42583668)

Email: contact@cashflowfinancial.com.au

Website: cashflowfinancial.com.au

We will respond to your enquiry or complaint and will work with you to resolve any concerns as quickly as possible.

Office of the Australian Information Commissioner (OAIC)

If you are not satisfied with our response to your privacy complaint, you may contact the OAIC:

Website: www.oaic.gov.au

Phone: 1300 363 992

Email: enquiries@oaic.gov.au

Post: GPO Box 5218, Sydney NSW 2001

Acknowledgment

This Privacy Policy has been updated to reflect the significant privacy law reforms introduced by the Privacy and Other Legislation Amendment Act 2024, which came into effect on 10 December 2024.

Key updates include:

- Enhanced disclosure requirements for automated decision-making systems (effective 10 December 2026)
- Strengthened security obligations with specific technical and organisational measures
- Expanded data breach notification obligations and procedures
- Comprehensive cross-border disclosure information, including details about overseas staff and cloud service providers
- Enhanced transparency about our information handling practices and infrastructure
- Clearer explanations of your rights under the Privacy Act

We remain committed to protecting your privacy and maintaining your trust. If you have any questions about these changes or how they affect you, please contact our Privacy Officer.

COOKIE NOTICE

By using our website, you acknowledge and agree to our use of cookies as described in this Privacy Policy. We use cookies to provide you with a great user experience and to help our website function effectively. For more information about cookies and how to manage them, please refer to Section 9 of this policy.