Privacy Policy ("Policy")

This Policy was last updated on 6 July 2026.

SuperGuardian (ACN 113 986 968) ('we', 'our', 'us', is bound by the Australian Privacy Principles (APPs) contained in the *Privacy Act 1988 (Cth)* (Privacy Act). This Policy explains how we collect, use store, disclose and protect your personal information, and how you can contact us about privacy matters.

While we may update our Policy from time to time. The most current version will always be available on our website. If we make any material changes, we will notify you by posting an updated version on our website and, where appropriate, contacting you directly via your nominated contact details.

If you have any questions, concerns, or complaints, please contact our Privacy Officer.

Privacy Officer: Joshua Williams

Email: joshua@superguardian.com.au

Postal address: GPO Box 1215, Adelaide SA 5001

Business Address: 65 Gilbert Street, Adelaide SA 5000

What information we collect

We may collect personal information directly from you, from third parties (such as service providers, regulators, or authorised representatives), and from publicly available sources where permitted by law. We collect this information to enable us to provide services, meet legal obligations, and manage our business operations.

At or before the time of collection (or as soon as practicable afterwards), we will take reasonable steps to ensure you are aware of:

- why we are collecting your personal information,
- how we may use and disclose it,
- the consequences if the information is not provided, and
- how you can access or correct your information.

In the course of providing our goods and services to you, we collect personal and other information about our clients, prospective clients, beneficiaries, trustees, directors, employees, contractors, service providers and other business contacts and how they interact with us, our goods, and our services. When you provide us with your personal information, you are agreeing to our collection and handling of your personal information in accordance with this Privacy Policy.

We collect personal information through a number of mechanisms, including:

- Contact details (name, address, email, phone number)
- Date of birth, occupation, dependants
- Identification documents (e.g. driver's licence)
- Tax File Number (TFN)
- Financial information (bank details, investments, superannuation)
- Business details (e.g. ABN)

You have the option of not identifying yourself or interacting with us using a pseudonym to make general inquiries about the goods and services that we offer, however, we will not be able to provide services to you without this information.

Information collected automatically

We may collect information through cookies and similar technologies, including:

- IP address and device information
- Browser and usage data
- Website interaction behaviour

Communications

We collect information when you communicate with us via email, phone, forms, or other channels.

Recruitment information

If you apply for a role, we may collect information from recruiters or job platforms to assess your application.

You may choose not to identify yourself in limited circumstances; however, this may prevent us from providing services.

How we use your information

We use personal information for purposes including:

- Providing and managing our services
- Identity verification and compliance obligations
- Client communication and support
- Financial administration and billing
- Internal reporting, analytics, and service improvement
- Legal and regulatory compliance

We may also use or disclose information where required or authorised by law or where you have provided consent.

Artificial Intelligence (AI) use

We may use secure artificial intelligence (AI) systems to assist with the delivery of our services, including data organisation, document processing, and service support functions.

Where AI systems are used:

- personal information is processed within controlled and secure environments;
- AI outputs are subject to human review and oversight;
- AI systems are not used to make sole automated decisions that produce legal or similarly significant effects;
- we do not use personal information to train public or externally accessible AI models; and
- we take reasonable steps to ensure personal information is not disclosed outside our organisation through AI processing.

Disclosure of personal information

We may disclose personal information to third parties including:

- Superannuation funds, insurers, and financial product providers
- Identity verification (DVS) providers
- IT, cloud, compliance, and professional service providers
- Legal and financial advisers (authorised representatives)
- Government and regulatory bodies where required by law
- Offshore support team members located in the Philippines, who are engaged under strict confidentiality obligations and contractual safeguards. We take reasonable steps to ensure overseas recipients handle personal information in a manner consistent with applicable privacy protections, however you acknowledge that overseas recipients may not be subject to the same privacy laws as Australia.

Storage, security and retention

We will take reasonable steps to protect the personal information we hold from misuse, loss, and unauthorised access, modification or disclosure. We do this by: ·

- Putting in place physical, electronic and procedural safeguards in line with industry standards;
- Requiring any third party providers to have acceptable security measures to keep personal information secure;
- Limiting access to the information we collect about you;
- Imposing confidentiality obligations on our employees;
- Providing privacy training (including on the appropriate use of systems) to those who are responsible for handling your personal information;
- Only providing access to personal information once proper identification has been given; and

When we store your data, we use industry-standard encryption technologies to protect personal information both at rest and in transit. This includes encryption of data stored in our systems using strong cryptographic controls (such as AES-256 or equivalent) and encryption of data transmitted over networks using secure protocols (such as TLS). Access to encrypted data is restricted to authorised personnel only and managed in accordance with our information security policies and recognised security frameworks.

While we take all steps reasonable in the circumstances to protect your information, in the unlikely event a data breach occurs, we will notify you in accordance with our obligations under the Privacy Act.

If we no longer require your personal information, and are not legally required to retain it, we will take reasonable steps to destroy or de-identify the personal information.

We retain personal information only for as long as it is required for the purposes for which it was collected, or as required by law. This may include retaining financial and transactional records for a minimum period required under taxation, corporate, or regulatory laws (including up to 7 years where applicable). After this period, information is securely destroyed or de-identified.

Security frameworks

SuperGuardian is committed to maintaining the confidentiality, integrity, and availability of personal information. We apply recognised information security frameworks, including:

- ISO 27001 (Information Security Management Systems)
- SOC reporting standards (where applicable)
- NIST Cybersecurity Framework

These frameworks guide our ongoing risk management, governance, and security controls, which are regularly reviewed and updated.

Document Verification Service (DVS)

We use the Australian Government's Document Verification Service (DVS) to verify identity information in accordance with applicable legal and regulatory requirements, including anti-money laundering and identity verification obligations.

You may choose not to provide identification; however, this may limit or prevent us from providing services to you where verification is required by law.

Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF)

SuperGuardian is a reporting entity under, and is subject to obligations imposed by, the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) (AML/CTF Act).

To comply with these obligations, we are required to undertake customer due diligence and may:

- collect and verify identification information (Know Your Customer (KYC) procedures);
- monitor transactions and client activity for suspicious or unusual behaviour;
- conduct ongoing customer due diligence (CDD);
- request additional information regarding source of funds or source of wealth; and
- report suspicious matters to the Australian Transaction Reports and Analysis Centre (AUSTRAC), where required by law.

We may be required by law to collect, use, and disclose personal information for AML/CTF compliance purposes without your consent.

Failure to provide requested information may result in delays in onboarding or the inability to provide services.

Where we engage third-party providers to assist with AML/CTF compliance, they are required to handle personal information securely and in accordance with strict confidentiality obligations.

Overseas disclosure

We may disclose personal information to overseas recipients, including our offshore team in the Philippines.

Where we do so, we take reasonable steps to ensure:

- The recipient handles information in accordance with applicable privacy and confidentiality obligations
- Appropriate contractual safeguards are in place
- Information remains secure and protected

Access and correction

You may request access to or correction of your personal information by contacting our Privacy Officer.

We will:

- Respond within 30 days where practicable
- Require identity verification before release
- Provide reasons if access is refused

We may charge reasonable administrative costs for providing access (excluding the request itself).

Complaints

If you believe we have breached your privacy rights, please contact our Privacy Officer in writing with details of your complaint.

We will:

- Acknowledge and investigate your complaint
- Respond within a reasonable timeframe
- Request identity verification where necessary

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

Office of Australian Information Commissioner (OAIC)
GPO Box 5288
SYDNEY NSW 2001
www.oaic.gov.au

Notifiable Data Breaches

In the event of a data breach that is likely to result in serious harm, we will:

- promptly assess and contain the breach;
- take remedial action where possible;
- notify affected individuals and the OAIC as required under the Notifiable Data Breaches scheme; and
- implement measures to reduce the likelihood of recurrence.

Notifications will be made as soon as practicable in accordance with our obligations under the Privacy Act.

Cookies and website analytics

We use cookies and similar technologies to support website functionality, improve user experience, and analyse website performance.

These technologies may collect information such as:

- IP address and device information,
- browser type and usage behaviour, and
- website interaction data.

We do not use cookies for third-party advertising or behavioural advertising purposes.
You can manage or disable cookies through your browser settings; however, some features of our website may not function correctly if cookies are disabled.

Privacy Impact Assessments

We may conduct Privacy Impact Assessments for high-risk activities involving personal information to identify and mitigate privacy risks.

Governing law

This Policy is governed by the laws of South Australia and the Commonwealth of Australia.