Privacy Policy for AML/CTF obligations

Our commitment

We are committed to protecting your privacy. We collect, use, share, process, and manage Personal Information only as reasonably necessary for carrying out our functions and activities.

If we prepare to provide, provide you with, or reasonably anticipate that we may provide you with, any Designated Services, we will handle your Personal Information provided in relation to those services in an open and transparent way, subject to our legal obligations, in accordance with this Privacy Policy.

What does this Privacy Policy cover?

This policy applies only to Personal Information handled in connection with our AML/CTF obligations under the AML/CTF Framework. Other parts of our legal practice may be outside the Privacy Act. We still handle that information confidentially under the legal profession legislation (as defined in section 3A of the *Legal Profession Uniform Law Application Act 2014* (NSW)), including the *Legal Profession Uniform Law Australian Solicitors' Conduct Rules 2015* (NSW).

Meaning of words used in this Privacy Policy

In this Privacy Policy the terms listed have the following meanings:

AML/CTF Act	*Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth).
AML/CTF Framework	AML/CTF Act, AML/CTF Rules and AUSTRAC-issued guidance.
AML/CTF Rules	*Anti-Money Laundering and Terrorism Financing Rules 2025* (Cth) made under the AML/CTF Act.
APP/s	The Australian Privacy Principles in Schedule 1 of the Privacy Act.
AUSTRAC	Australian Transaction Reports and Analysis Centre.
Designated Services	All the services described as Professional Services in Table 6 of section 6 of the AML/CTF Act and its relevant subsections, including: • Assisting a person to plan, execute, or act on their behalf to buy, sell, or transfer real estate (unless ordered by a court or tribunal). • Assisting a person to plan, execute, or act on their behalf to buy, sell, or transfer a body corporate or legal arrangement (unless ordered by a court or tribunal).

	• Receiving, holding, controlling, or managing a person's money while assisting them with, or acting on their behalf in, a transaction. • Selling or transferring a shelf company. • Assisting a person to plan, execute, or act on their behalf in the creation or restructuring of a body corporate or legal arrangement.
We, us, our	McAulay Hesford Lawyers Pty Limited ABN 69 648 615 703, practising as Highlander Law.
KYC Information	Information sufficient to: i. establish initial customer due diligence matters on reasonable grounds as required by; or ii. fulfil our ongoing customer due diligence obligations under the AML/CTF Act. including: • the identity of our customer; • the identity of any person on whose behalf our customer is receiving the service; • the identity of any person acting on behalf of the customer including their authority to act; • if the customer is not an individual, the identity of any beneficial owners; • whether the customer, beneficial owner, or any person acting on their behalf is a politically exposed person or a person designated for targeted financial sanctions; • information regarding source of wealth and source of funds; • the nature and purpose of the business relationship or transaction; and • any other matter specified in the AML/CTF Rules. This may include identification documents (such as passports or driver licences), electronic verification information, screening results (including sanctions and politically exposed person checks), and other information used to verify your identity.
OAIC	Office of the Australian Information Commissioner.
Personal Information	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, provided to us for the purposes of, or in connection with, activities relating to the AML/CTF Act or regulations or AML/CTF Rules.
Privacy Act	*Privacy Act 1988* (Cth).
Sensitive Information	(a) Personal Information that includes information or an opinion about an individual's: i. racial or ethnic origin; or ii. political opinions; or iii. membership of a political association; or iv. religious beliefs or affiliations; or v. philosophical beliefs; or vi. membership of a professional or trade association; or vii. membership of a trade union; or viii. sexual orientation or practices; or ix. criminal record; or (b) health information about an individual; or (c) genetic information about an individual that is not otherwise health information; or (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or (e) biometric templates.

What privacy law applies to our relationship

We are a "small business operator" under s 6D of the Privacy Act and become subject to the Privacy Act, for the first time, only in relation to AML/CTF-related activities by operation of s 6E(1A) of that Act.

Accordingly, the Privacy Act, including the APPs, applies only to our collection, use, sharing, processing, and management of Personal Information required to comply with our obligations under the AML/CTF Framework.

Under APP 2 you may interact with us anonymously, or using a pseudonym, where lawful and practicable. However, interacting anonymously or using a pseudonym is not possible where we are required to verify identity under the AML/CTF Framework.

How do we collect Personal Information?

We collect Personal Information only by lawful and fair means.

We will collect Personal Information directly from the individual who is the subject of the information unless:

- the individual has consented to collection of his or her Personal Information from a third party,
- it is unreasonable or impractical to make a direct collection; and/or
- we are required or authorised by law to collect his or her information from a third party.

We may collect Personal Information when you, your organisation, or those acting on your or your organisation's behalf:

- visit us or meet with our representatives;
- communicate with us, including by physical post, email, social media, telephone or text message;
- register to attend, present at or otherwise participate in a meeting, conference or event hosted or presented by us; and/or
- engage us to provide services including when you supply KYC Information in response to our direct request.

If we use a credit reporting body for electronic identity verification, we will seek your express consent prior to doing so and offer an alternative means of verification (for example, certified copies of identification documents), as legally required.

We will provide you with a collection notice at or before the time we collect your Personal Information.

What Personal Information do we collect?

We are required by law under the AML/CTF Act to collect and verify certain Personal Information and may be prohibited from providing services if we cannot do so.

In particular, we collect KYC Information as required by the AML/CTF Act which may include: names, addresses, contact details, job titles, services and transactions obtained, offered and supplied including usage history, including information about the time, place, and circumstances of our interactions with you.

We may infer information about you from your engagement with us and your activities. We may also collect Sensitive Information where required for compliance with the AML/CTF Framework or where otherwise permitted by law.

We may conduct ongoing monitoring of transactions and client information to comply with our AML/CTF obligations.

What happens if you don't provide us with requested Personal Information?

If you do not provide requested Personal Information, we may be unable to provide Designated Services and/or comply with our legal obligations.

Purposes of collection of Personal Information

We collect and use Personal Information to carry out our activities and functions including providing you with Designated Services, complying with our regulatory obligations in relation to the delivery of those services, including adherence to the *Legal Profession Uniform Law* and its related rules and legislation, the *Legal Profession Uniform Law Australian Solicitors' Conduct Rules 2015* (NSW) and the *Legal Profession Uniform General Rules 2015* (NSW).

Other relevant legislation which may require us to collect and use your Personal Information includes the *Duties Act 1997* (NSW) and the Australian Registrars National Electronic Conveyancing Council's Model Participation Rules.

Unless you consent to us doing so otherwise, we will only use your Personal Information for the primary purpose for which it was collected, and for any secondary purpose if you would reasonably expect, and the purpose is related to, the primary purpose of collection. Examples of secondary purposes you might reasonably expect are listed in the previous paragraph.

In the case of Sensitive Information, any secondary purpose will be one that you would reasonably expect and directly related to the primary purpose of collection.

Disclosure of Personal Information

Third parties

Subject to legal requirements, we do not share your Personal Information with any third parties except:

- with your express permission; and
- to contracted service providers to organise or facilitate the efficient and effective administration, management or delivery of our services. This may include service providers that support our due diligence processes associated with complying with our AML/CTF obligations.

We will ensure that such service providers commit to protecting your Personal Information appropriately and agree not to use or disclose your Personal Information for any other purpose (other than as required by law).

Legal requirements

We may use or disclose your Personal Information in circumstances where required by law and/or expressly permitted by the *Privacy Act,* including if:

- it is not reasonable or practical to obtain consent and we reasonably believe use or disclosure is necessary to lessen or prevent a serious threat to life, health, or safety of any individual or public health and safety;
- we have reason to suspect that unlawful activity or misconduct of a serious nature that relates to our activities or functions is being or has been engaged in, and we believe the collection, use or disclosure is necessary to take appropriate action in relation to the matter;
- we reasonably believe that the collection, use or disclosure is reasonably necessary to assist with the location of a person reported missing; or
- we are compelled by law including:
    - by warrant or subpoena;
    - where we are required by request under statute or lawful order of a government agency or authority including law enforcement, courts and tribunals and regulators; and/or
    - to AUSTRAC and other government agencies without your knowledge or consent, including where we form a suspicion about a matter or transaction under the AML/CTF Framework.

Nothing in this Privacy Policy limits our obligations of confidentiality or client legal privilege. However, there may be circumstances where we are compelled to disclose confidential information to AUSTRAC under the AML/CTF Framework.

We are prohibited from notifying you of disclosures to AUSTRAC and may be prohibited from notifying you of disclosures to other government agencies or authorities.

Business transactions

If we are involved in a merger, acquisition or asset sale, your Personal Information may be disclosed in confidence as part of a due diligence process and may be transferred to the new owner. We will provide notice before your Personal Information is transferred and becomes subject to a different Privacy Policy.

How do we protect your information?

We hold Personal Information in hard copy and electronic formats. We take reasonable steps to prevent unauthorised access, disclosure, alteration, destruction or loss of Personal Information including by using a range of physical, operational and technological security measures to protect this information. These measures include organisational and technical measures such as:

- staff education and training to ensure our staff are aware of their privacy obligations when handling your Personal Information;
- technological security measures, including firewalls, encryption and anti-virus software.

Where a data breach is likely to result in serious harm, we will comply with the Notifiable Data Breaches scheme in the Privacy Act, including notifying the OAIC and affected individuals, as required.

When we consider that Personal Information is no longer needed for any purpose for which the information may be used or disclosed in accordance with this Policy and that we are not required by law or court order to retain the Personal Information, we will take reasonable steps to destroy or de-identify the information. AML/CTF KYC Information and transaction records are kept for seven years after the business relationship ends or the transaction is completed, as required by the AML/CTF Framework.

Can your Personal Information be accessed offshore?

We maintain your Personal Information physically and electronically within Australia where possible unless we have agreed with you to share your Personal Information with third parties offshore (such as local experts in another jurisdiction). This includes cloud-based practice management systems, search platforms and compliance service providers used in connection with our AML/CTF obligations.

Some electronic services we use may process data offshore however we limit this and maintain data processing in Australia wherever possible.

We take reasonable steps to ensure overseas recipients do not breach the APPs.

How you can access and correct your Personal Information

We will respond to inquiries from an individual regarding whether we hold any Personal Information relating to that individual and will allow access to and correction of any such Personal Information subject to our contractual arrangements where Personal Information is held by a third party, and the conditions and limitations set out in the Privacy Act, including:

- if we reasonably believe that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety;
- giving access would have an unreasonable impact on the privacy of other individuals;
- the request for access is frivolous or vexatious;
- the information relates to existing or anticipated legal proceedings between the organisation and the individual, and would not be accessible by the process of discovery in those proceedings;
- giving access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations;
- giving access would be unlawful;
- denying access is required or authorised by or under an Australian law or a court/tribunal order;
- the organisation has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the organisation's functions or activities has been, is being or may be engaged in and giving access would be likely to prejudice the taking of appropriate action in relation to the matter;
- giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or
- giving access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process.

If you believe that the Personal Information we, or our contracted third party, hold about you is inaccurate, out-of-date, incomplete, irrelevant, or misleading, you may request that we correct it by contacting our Privacy Officer. We may ask you to verify your identity before giving you access or making corrections, and we may charge a reasonable fee for providing access (but not for making a correction).

You can contact our Privacy Officer by email at office@hlaw.au

We will take reasonable steps to correct your information to ensure it is accurate, complete, and up-to-date within a reasonable period (usually within 30 days) of receiving your request.

How you can complain about our information handling practices

All privacy-related inquiries and complaints are handled by our Privacy Officer. If you have any concerns regarding our management of your Personal Information, or if you believe we have breached the APP/s, please contact our Privacy Officer in writing setting out the details of your complaint.

We are committed to achieving a fair and equitable resolution of any privacy concerns. When you lodge a complaint, we will follow this internal review process:

1. We will acknowledge receipt of your written complaint within a reasonable time (usually within seven days).
2. Our Privacy Officer will conduct an internal investigation into your complaint. This will involve reviewing the circumstances of the collection, use, or disclosure of your information and assessing our compliance with our internal procedures and the Privacy Act. We may contact you to request further information to assist with our investigation.
3. We will endeavour to complete our investigation and provide you with a written response outlining the outcome of our review, our decision, and any corrective actions we propose to take within 30 days of receiving your complaint.

If you are not satisfied with our response, or if we do not resolve your complaint within 30 days, you are entitled to escalate your complaint by lodging a complaint with the Office of the Australian Privacy Commissioner at this link: https://www.oaic.gov.au/privacy/privacy-complaints/lodge-a-privacy-complaint-with-us.

If you require a copy of this Privacy Policy in a particular form (e.g. large print, accessible PDF) please contact our Privacy Officer.

Date reviewed: 18 June 2026.