



Queensland
Law Society®

Toowong Legal Privacy Policy

How to use this template.

This template policy is intended exclusively for small law practices which:

- Have an annual [turnover less than 3 million dollars](#); and
- provide ‘designated services’ under the AML/CTF Act.

Such an entity is a “small business” and not all data collected and held by it will be *Privacy Act* 1988 (Cth) (**Privacy Act**) regulated. Where an organization within the small business exemption collects “personal information” after 1 July 2026, only that component collected or held “for the purposes of or in connection with” the AML/CTF Act obligations, falls within Privacy Act obligations. This template policy has been drawn with that limitation in mind.

The [OAIC’s Privacy Guidance for reporting entities under the AML/CTF Act](#) explains the legislative schema.

It **may** be more efficient for your firm to treat all the information you hold as if it were Privacy Act regulated and not attempt to apply different processes. However, your Privacy Policy, Retainer Agreement and Collection notices¹ should not accidentally extend your regulatory obligations unless this is a considered decision.

This document is a template, and as such is no more than a starting point for the policy that your firm will ultimately adopt. It is important that you read the guidance, consider what *regulated data* your firm will collect and hold, then modify the policy accordingly.

The firm’s Privacy Policy (and key provisions) should also be incorporated into the terms of the retainer by reference.

It is important to note that the usual confidentiality obligations which apply to clients, court and counterparties are unaffected. Confidentiality and professional obligations which have always applied will continue to do so.

Extraterritorial legislation such as the [GDPR](#) may apply to law firm operations in Australia. This policy has not been written to comply with such foreign legislation.

Artificial Intelligence (AI)/Automated Decision Making (ADM): This template does not include statements about ADM. With effect from 10 December 2026, your firm’s use of personal information for certain ADM outcomes will require privacy policy disclosures under Australian Privacy Principles (APPs) 1.7-1.9 to the extent your firm must make any privacy policy disclosures under the APPs. In any event your firm’s use and disclosure of personal information in connection with AI/ADM involves considerations about client consents, professional standards and various courts’ rules which are outside the scope of this template.

Each issue which must be dealt with is described simply in the initial paragraph with further detail (where needed based on the firm’s specific circumstances), elaborated in the “Long-form additions” box.

“**Drafting notes**” in blue panels are intended to be deleted prior to adoption.

¹ The OAIC has published a Template privacy collection notice for reporting entities under the AML/CTF Act here <[Template privacy collection notice for reporting entities under the Anti-Money Laundering and Counter-Terrorism Financing Act | OAIC](#)>.

Privacy Policy

1. Introduction

Toowong Legal ABN 71 357 112 668 are referred to in this Privacy Policy as **we, us or our**.

This Privacy Policy explains how we manage personal information. It also describes your rights to access and correct personal information we hold about you, and how you can make a complaint about our management of your personal information. This is in addition to our obligations of confidentiality to clients and other parties arising from sources other than the Privacy Act.

1.1. Application of this Policy

This Privacy Policy only applies to some of the personal information we manage. It only applies to personal information we manage for the purposes of or in connection with our obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (the **AML/CTF Act**)

Other personal information we manage remains excluded by applicable exemptions in the Privacy Act.

1.2. Related Entities

References to Toowong Legal in this Privacy Policy include related entities. For more information see:

- **Not Applicable**

1.3. Policy Updates

Drafting note

When making substantial Privacy Policy Updates, firms should consider whether they have an obligations to formally notify clients of the changes.

We may update this Privacy Policy from time to time to reflect changes in our practices or legal requirements. The current version will be available on our website at www.toowonglegal.com.au.

2. Personal information: what we collect

Types of personal information We collect your contact and identity details, financial information and case related information about you and any relevant entity or person. This may include sensitive information. **Long form additions:**

The types of personal information we may collect includes:

- **Identity information:** name, date of birth, gender, signature, photographic identification, offices or directorships held;
- **Contact information:** residential and postal addresses, email addresses, telephone numbers;
- **Professional and business information:** occupation, employer, job title, professional qualifications, business holdings and structures;
- **Financial information:** bank account details, billing information, payment card details, tax file numbers*;
- **Matter-related information:** information relevant to your legal matter or the legal matter of our client;
- **Transaction information:** details of services provided to you or your organisation;

- **Communication records:** records of correspondence and communications with you;
- **Website and technical data:** IP address, browser type, device information, pages visited, cookies (see section 8);
- **Recruitment information:** employment history, qualifications, references, right to work status, background check results; and
- **Sensitive information:** including: sexual orientation, racial and ethnic origin, political beliefs, religious affiliation, criminal record, and health information.

*Firms should consider if collection of tax file numbers is mandated in a way that its management will not contravene the [Privacy \(Tax File Number\) Rule 2015](#), see OAIC guidance [here](#).

2.1. Identity Verification and the AML/CTF Act

We may be required to verify your identity and collect certain information under the AML/CTF Act when we provide designated services. Identity documents might also be required for other services such as court matters, real property transactions and asset dealings.

This includes collecting identification documents and information about the source of funds and beneficial ownership of entities.

3. How we collect personal information

3.1. Sources of information

We collect information directly from our clients, from other lawyers, government sources or public sources such as registers or the internet.

Long form additions:

1.1 Direct Collection

Where reasonable and practicable, we collect personal information directly from you. This may occur when you:

- engage us to provide legal services;
- respond to communication with us or engage a solicitor or agent to do so;
- contact us by telephone, email, post or in person;
- complete forms or provide documents to us;
- visit our website or use our online services; or
- apply for employment with us.

1.2 Indirect Collection

We may also collect personal information about you from third parties, including:

- our client(s), where we collect information in the course of providing legal services;
- other parties to legal proceedings or transactions and their lawyers;
- witnesses of fact, expert witnesses, health care providers and hospitals;
- courts, tribunals, law enforcement and government agencies;
- publicly available sources, including public registers, websites and social media;
- referrers who introduce you to us or lead agencies and advertising sites;
- recruitment agencies and previous employers (for job applicants); and
- identity verification, commercial data brokers and background check service providers.

3.2. Anonymity and Pseudonymity

If you are a client, you have the option of requesting to deal with us anonymously or by using a pseudonym. However, in most cases this is not lawful nor practical for legal services. If you do not provide us with the personal information we request, we may not be able to provide you with legal services or respond to your enquiry.

4. Why we collect personal information and how we use it

We collect, hold, use and disclose personal information for the primary purpose of providing legal services to our clients, complying with regulatory and insurance obligations and operating our legal practice.

Secondary purposes include financial management, system improvement, enforcement of our right to payment and managing the relationship between our firm and former clients once the retainer has concluded.

Long form additions:

Collection purposes

1.1. Primary Purposes

This includes:

- providing legal advice and representation to you or to our client(s);
- managing client matters and files;
- conducting legal research and investigations;
- preparing and reviewing legal documents;
- communicating with you and other parties;
- billing and collecting fees, including pursuit of our rights under a Costs Agreement or retainer;
- complying with our legal, professional and insurance obligations; and
- administering and managing our firm.

1.2. Secondary Purposes

We may also use and disclose personal information for secondary purposes that are related to our primary purposes, including:

- maintaining and developing our relationship with you;
- quality assurance and improvement of our services, including training our AI models or those of our AI providers (subject to our obligations of confidentiality to you);
- training and professional development;
- ongoing Customer Due Diligence as required by the AML/CTF Act;
- training AI or automated systems including AI development by our vendors with appropriate confidentiality safeguards in place;
- enforcement of our right to payment of fees;
- internal reporting and analysis; and
- risk management and insurance purposes.

5. Disclosure of Personal Information

We may disclose personal information to third parties to facilitate the purposes of collection noted in section 4. These purposes include disclosure to parties to proceedings or transactions and their representatives, to Courts, government and regulatory agencies as may be necessary or appropriate to establish legal rights and to progress transactions in which we are instructed. We also disclose information to third parties (such as data storage or archiving companies, our regulators or our insurers) who hold or process information for us.

Long form additions:

Your personal information and confidential data is held by us subject to our duty of confidentiality under the Australian Solicitor's Conduct Rules ("**ASCR**") and any applicable undertakings or court rules. We may disclose personal information to third parties subject to those obligations and for the purposes described in this Privacy Policy, including:

- to discharge our professional obligations to you or to our clients or in the reasonable execution of our instructions;
- to comply with our legal obligations or in answer to a compulsory notice such as a subpoena or warrant, or to disclose information under the AML/CTF Act, Criminal Code(s), *Legal Profession Act* or other relevant legislation;
- to barristers, mediators, expert witnesses, investigators and consultants and other legal practitioners engaged to act for you (and/or our client) or in relation to the matter;
- other parties to legal proceedings or transactions as instructed, reasonably necessary or required by law;
- courts, tribunals, government agencies and regulators;
- our professional indemnity insurers;
- a Costs Assessor in the event that an assessment is ordered or reasonably necessary.
- service providers who assist us to operate our business (including IT providers, AI providers, document management providers, and marketing service providers);
- related entities;
- as permitted under the ASCR confidentiality exceptions; and
- any person you expressly or impliedly authorise us to disclose information to.

6. Overseas Disclosure

We will disclose information to overseas recipients where this is reasonably necessary to progress our instructions (dealing with a company with an overseas office, for example).

We may disclose personal information to recipients located outside Australia where reasonably necessary or convenient to facilitate the purposes of collection, holding, use and disclosure of information stated in sections 2 and 5 of this policy.

Long form additions:

- The following circumstances are common examples when that may apply:
- where your matter involves overseas parties or overseas proceedings;
- to overseas law firms or legal practitioners engaged in a matter;
- to our staff, staff of a related entity or contractors if working or travelling overseas;
- to parties such as regulators and auditors who may use overseas processors or offices;
- to service providers whose systems or servers are located overseas (including cloud

storage, AI and IT service providers if we consider that the confidentiality arrangements that will apply to such information is sufficient); and

- where you instruct or authorise us to do so.

Cross-border disclosure of personal information

Countries where personal information may be disclosed include: Not Applicable

7. Security of Personal Information

7.1. Security Measures

We hold your personal information using a system designed to protect against data breaches, however like all data security systems, risks may only be mitigated but not eliminated. It is our practice to require our storage service providers to be reputable [and to seek assurances from them regarding security and confidentiality].

7.2. Retention and Destruction

We retain personal information for as long as necessary to fulfil the purposes for which it was collected, to comply with our legal and professional obligations and to ensure that pertinent evidence remains available if reasonably required.

8. Third party websites

Our website may contain links to third party websites, such as payment processors. We are not responsible for the privacy practices of those websites, and we encourage you to read their privacy policies.

9. Access and Correction

9.1. Access to and correction of your Personal Information

You have the right to request access to or correction of the personal information we hold about you. To make an access request, please contact our Privacy Officer (see Section 10).

If we refuse to correct your personal information, we will provide written reasons for the refusal and information about how you may complain.

The Privacy Act permits us to refuse access in some circumstances. If we refuse your access request, we will provide you with written reasons for the refusal (unless unreasonable to do so or we are prohibited from doing so by law) and information about how you may complain.

Long form additions:

Access and correction

- We will respond to your request within a reasonable period, generally within 30 days. We may charge a reasonable fee to cover the costs of locating, retrieving and providing the information. If you are a client or former client we do not charge for recovery or storage of records that are your property, but may charge for costs incurred in retrieval of other records or where urgent timelines or requests for documents to be delivered remotely, incur additional outlays.
- If you are not a client or former client, our confidentiality obligations to them and other relevant exemptions under the Privacy Act may preclude us giving you the information requested. Request for search or recovery costs in advance does not mean that information will necessarily be released. We will inform you of any applicable fees before processing your request.

Correction of Your Personal Information

- We take reasonable steps to ensure that the personal information we hold during the currency of your matter is accurate, up-to-date, complete and relevant. Records held subsequent to the completion of our work for you will not be monitored or updated unless further instructions are issued. If you believe that personal information we hold about you is inaccurate, out-of-date, incomplete, irrelevant or misleading, you may request that we correct it.
- We will respond to correction requests within a reasonable period. If we correct information that we have previously disclosed to a third party, we will notify that third party of the correction if you request us to do so.

10. Complaints and questions

If you have a question about this policy or complaint about how we have handled your personal information, please contact our Privacy Officer. We ask that you provide details of your complaint in writing. We will acknowledge your complaint within 7 business days and investigate it promptly. We aim to resolve complaints within 30 days. If we need more time, we will keep you informed of our progress.

Privacy Officer

Neville James White, Principal

You may also contact the relevant legal services regulator in your State or Territory.

Long form additions:

Privacy officer details and complaints

Toowong Legal

Address: PO Box 85, Toowong Qld 4066

Email: jwl@toowonglegal.com.au

Phone: 07 3870 8043

If you are not satisfied with our response, you may escalate your complaint to:

Office of the Australian Information Commissioner (OAIC) or the Legal Services Commission.

Website: www.oaic.gov.au

Phone: 1300 363 992

Email: enquiries@oaic.gov.au

Post: GPO Box 5218, Sydney NSW 2001

Version	Date	Change Log
Template	XX/XX/26	--

Ver 1.--	210626	First Draft
----------	--------	-------------

--- End of Privacy Policy ---