

Privacy Policy



Effective date: September 2026

1. General

In this Privacy Policy (Policy), “we”, “us” and “our” mean Nolan & Lu Limited trading as Nolan & Lu Lawyers.

We are a New Zealand law firm. This Policy explains how we collect, hold, use and disclose personal information and how we meet our obligations under the Privacy Act 2020 (Act), including the information privacy principles (IPPs). It also explains how you may ask to access or correct personal information we hold about you.

This Policy applies to personal information relating to clients, prospective clients and other individuals we deal with in the course of our practice and business. Separate arrangements may apply to employees, contractors and job applicants.

Nothing in this Policy limits any legal or professional obligation that applies to us, including obligations relating to legal professional privilege, confidentiality, court orders, statutory restrictions, or the Lawyers and Conveyancers Act 2006 and applicable professional conduct rules.

2. What is personal information?

Personal information is information about an identifiable individual. Whether information is personal information depends on whether an individual is identifiable from the information itself or together with other information reasonably available.

You may choose not to provide personal information unless its provision is required by law. However, if we do not receive information we reasonably need, we may be unable to act for you, continue acting for you, provide a service, complete a transaction, comply with legal obligations, or respond to a request.

3. What personal information may we collect?

The information we collect depends on the circumstances. It may include:

- identity information, such as your name, date of birth, occupation, signature, photograph, passport, driver licence, birth certificate or other identification;
- contact information, such as residential, postal and email addresses and telephone numbers;
- immigration, citizenship or residency information where relevant to the services requested;
- unique identifiers, such as passport numbers, driver licence numbers, IRD numbers or other identifiers where lawfully required or reasonably necessary;
- financial information, including billing information, payment details, bank account details, source of funds or source of wealth information where relevant;
- information required for client due diligence, sanctions, fraud prevention, conflict checking or other legal and professional compliance purposes;
- information about your legal, commercial, family, employment, property, business or other affairs that is relevant to an enquiry or matter;
- communications with you and records relating to the services we provide;
- information about another person where you provide it to us or where we lawfully collect it from another source;
- website and technology information, such as IP address, device or browser information, cookies and website usage information; and

- any other personal information that is reasonably necessary for a lawful purpose connected with our functions or activities.

4. When and how do we collect personal information?

4.1 Collection from you

We may collect personal information directly from you when you contact us, make an enquiry, instruct us, provide documents or information, enter into a transaction or other arrangement with us, use our website or online services, attend an event, communicate with us, or otherwise deal with us.

Where IPP 3 applies, we will take such steps as are reasonable in the circumstances to make you aware of the matters required by IPP 3. Those steps may be taken through this Policy, an engagement letter, a form, a notice, correspondence or another appropriate means. We are not required to repeat those steps where an exception in IPP 3 applies, including where we have recently provided the same information in relation to the same or similar collection.

4.2 Collection from other sources

We will ordinarily collect personal information from the individual concerned where required by IPP 2. We may collect information from another source where permitted by the Act or another law, including where an applicable exception to IPP 2 applies.

Depending on the matter, other sources may include:

- your representatives, agents, advisers, employers, employees, family members, counterparties, witnesses or other people involved in a matter;
- public registers and publicly available sources, including the Waka Kotahi (NZTA), Department of Internal Affairs, Companies Register, Personal Property Securities Register and other lawful public sources;
- courts, tribunals, government agencies, regulators, law enforcement bodies or local authorities;
- banks, financial institutions, insurers, credit reporting or verification providers;
- client due diligence, identity verification, sanctions-screening or fraud-prevention providers; and
- other persons or organisations where collection is authorised by you or permitted by law.

4.3 Notification of indirect collection - IPP 3A

For personal information collected on or after 1 May 2026 from a source other than the individual concerned, where IPP 3A applies and no exception applies, we will take such steps as are reasonable in the circumstances to ensure the individual is aware of the matters required by IPP 3A. This includes the fact and purpose of collection, intended recipients, the identity and address of the collecting and holding agency, any law authorising or requiring the collection where applicable, and rights of access and correction.

We are not required to provide an IPP 3A notification where an exception in the Act applies. For example, depending on the circumstances, an exception may apply where the individual has already been made aware of the required matters, non-compliance would not prejudice the individual's interests, notification would prejudice the purpose of collection or specified legal functions, notification is not reasonably practicable, or the information will not be used in an identifiable form. We may rely on any applicable statutory exception.

5. Why do we collect and use personal information?

We may collect and use personal information for lawful purposes connected with our functions and activities, including to:

- respond to enquiries and determine whether we can act;

- identify clients and other relevant persons and conduct conflict checks;
- provide legal services, advice and representation and manage client matters;
- communicate with clients and other persons involved in a matter;
- verify identity and comply with legal and professional obligations, including obligations under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 where that legislation applies to the relevant service or activity;
- manage trust account, billing, payment, accounting and debt recovery functions;
- prevent, detect and respond to fraud, cyber security incidents, unlawful conduct and risks to our systems or services;
- administer and improve our practice, systems, website, services and business operations;
- manage complaints, disputes, insurance, audits, regulatory enquiries or legal proceedings;
- send publications, invitations or marketing communications where permitted by law, with applicable unsubscribe options; and
- use information for another purpose where permitted by the Act or other law.

We will not use personal information for another purpose unless that use is permitted by IPP 10 or other applicable law.

6. Who may we disclose personal information to?

We may disclose personal information where permitted by the Act, authorised by the individual, necessary for the provision of legal services, required or authorised by law, or otherwise permitted by our legal and professional obligations. Depending on the circumstances, recipients may include:

- our partners, directors, employees, contractors and other personnel who need the information for their work;
- barristers, other lawyers, experts, mediators, arbitrators, investigators, process servers, consultants and other professional advisers or service providers engaged in connection with a matter;
- courts, tribunals, regulators, government agencies, law enforcement bodies and other persons where disclosure is required or permitted by law;
- banks, financial institutions, insurers, auditors, accountants, trust account providers and payment service providers;
- identity verification, client due diligence, sanctions-screening, fraud-prevention, credit reporting or debt recovery providers;
- IT, software, document management, cloud hosting, data storage, cyber security, communications, archiving and confidential destruction providers;
- counterparties and their advisers, where disclosure is necessary or appropriate for the matter and permitted by our duties; and
- any person you authorise us to disclose information to.

We will disclose personal information only where there is a lawful basis to do so. Our handling of client information is also subject to applicable duties of confidentiality and legal professional privilege.

7. Overseas storage, processing and disclosure

Personal information may be stored or processed using service providers located in New Zealand or overseas. Where an overseas provider stores or processes personal information solely as our agent and does not use the information for its own purposes, the transfer may be treated under the Act as information held by us rather than a disclosure to the provider.

Where we disclose personal information to a foreign person or entity and IPP 12 applies, we will comply with the applicable requirements of IPP 12. Depending on the circumstances, this may include being satisfied on

reasonable grounds that the recipient is subject to the Act or comparable privacy safeguards, using contractual safeguards, obtaining the individual's authorisation after providing the notice required by IPP 12, or relying on another basis permitted by law.

We use cloud data storage services from Dropbox and their privacy policy can be accessed at dropbox.com/privacy

We do not promise that every overseas recipient is subject to New Zealand law. Where IPP 12 applies, we will use a permitted basis for the disclosure.

8. Website, cookies and analytics

Our website may use cookies or similar technologies. Cookies are small data files stored on or accessed from your device. They may be used to operate the website, remember preferences, understand website usage, maintain security or improve services.

You can usually configure your browser to block or delete cookies. If you do so, some website functions may not operate as intended.

We may use aggregated or de-identified website usage information for analytics and business purposes. Where information remains personal information, this Policy applies.

9. Direct marketing

We may use contact details to send legal updates, publications, invitations or other communications where permitted by law. You may ask us to stop sending marketing communications at any time by using an unsubscribe facility, if provided, or contacting us. This does not prevent us from sending communications that are necessary for an existing matter, relationship or legal obligation.

10. Security and storage

We may hold personal information electronically or physically, at our premises or using third-party systems or storage providers in New Zealand or overseas.

We will use such security safeguards as are reasonable in the circumstances to protect personal information against loss, unauthorised access, use, modification or disclosure and other misuse, as required by IPP 5. The safeguards used may vary depending on the sensitivity of the information, the circumstances and the systems involved.

Where a service provider holds or processes personal information on our behalf, we will take reasonable steps appropriate to the arrangement to address confidentiality and security obligations.

11. Retention and disposal

We will not keep personal information for longer than is required for the purposes for which the information may lawfully be used, subject to any legal, professional, insurance, record-keeping, evidential or other lawful requirements that apply. When information is no longer required, we may securely destroy, delete or de-identify it. We are required by law to retain client files and documents for 7 years, which we may do so either electronically or physically.

12. Privacy breaches

If a privacy breach occurs, we will assess and respond to it in accordance with the Act. Where it is reasonable to believe that the breach has caused serious harm to an affected individual or is likely to do so, we will notify the Privacy Commissioner as soon as practicable after becoming aware that the breach is notifiable, as required by the Act.

We will also notify affected individuals as soon as practicable where required by the Act, subject to any statutory exception allowing notification to be delayed or withheld. If direct notification is not reasonably practicable and the Act requires public notice, we will give public notice in the manner required by the Privacy Regulations 2020.

13. Access to and correction of personal information

You may ask us to confirm whether we hold personal information about you and, subject to the Act, request access to that information. You may also request correction of personal information you believe is incorrect.

Requests should be made to our Privacy Officer using the contact details at the beginning of this Policy. We may ask for information reasonably necessary to verify your identity or authority before responding.

We will respond within the time required by the Act. We may refuse or limit access where the Act permits or requires us to do so. Other legal obligations or rights may also affect what can be provided, including legal professional privilege, duties owed to other clients or persons, court orders, statutory restrictions and professional obligations.

If we do not make a requested correction, you may ask us to attach to the information a statement of the correction sought, as provided by the Act.

Any charge for an access request will only be made where permitted by the Act or other applicable law.

14. Privacy Officer and complaints

We have appointed one or more Privacy Officers as required by the Act. Our Privacy Officer can be contacted using the details at the beginning of this Policy.

If you have a privacy concern or complaint, please contact our Privacy Officer. We will consider the issue and respond as appropriate.

You may also make a complaint to the Office of the Privacy Commissioner. Current contact information is available at www.privacy.org.nz or on 0800 803 909.

15. Changes to this Policy

We may amend this Policy from time to time. The current version will be made available through our usual publication method, such as our website. Changes take effect from the effective date stated in the updated Policy.

16. Contact details

For access or correction requests, privacy questions or complaints, contact us at privacy@notanlulawyers.co.nz or (07) 834 0365.