PRIVACY POLICY

Table of Contents

1 Introduction

1.1. This Privacy Policy outlines our obligations to manage the personal information we hold about our clients (prospective and actual), workers, suppliers and others.

1.2. It applies to information provided to us so we can tailor our legal practice management software services for our clients, and also to when our website, practice management and other applications and services are used and accessed.

1.3. We respect and value the information shared with us and will follow the Privacy Act 2020 in relation to it.

1.4. This Privacy Policy will be supplemented by additional privacy statements, terms and notices from time to time, as well as our Data Protection Policy.

1.5. In this Policy, **information** generally means any information which relates to an individual including that which can be used as a means of identification of that individual. Examples of this are included under Part 5 of this Policy.

2. Purpose

2.1. This Policy provides guidance on how OneLaw and its workers and leadership will comply with the requirements set out in the Privacy Act 2020 and its commercial client contracts relating to the collection and management of information provided to, used, and held by, OneLaw.

3. Why do we collect Information?

3.1. OneLaw will only collect information through transparent, fair and lawful means. It will only be used to satisfy our business functions and activities.

3.2. OneLaw may collect, use and hold information through a variety of means, including OneLaw sites or services, employment and contractor processes, and contact with OneLaw representatives during the marketing or purchase of our services. Part 6 of this Policy provides further examples of such means.

3.3. We collect information to:

(a) Market and sell our services.

(b) Process and act on instructions from our clients for our legal practice management services.

(c) Verify identity.

(d) Provide relevant information.

(e) Analyse and improve our legal practice management services.

(f) Streamline and personalise our client experience while dealing with OneLaw.

(g) Meet our legal obligations and facilitate our internal business operations.

(h) Assess whether or not to engage workers and suppliers and how to deal with them once engaged.

(i) Respond to any issues regarding any of our legal practice management services.

3.4. All of us here at OneLaw need to take all reasonable steps to check that the information we collect, use, hold and disclose is accurate, complete, relevant, not misleading and up to date. If anyone at OneLaw becomes aware that any of the information we hold does not meet these standards, they are to rectify that or immediately discuss it with our Privacy Officer.

4. Whose Information do we collect?

4.1. We collect information about:

(a) Our current and prospective clients and business associates.

(b) Suppliers.

(c) Employees, contractors and leadership (current and prospective).

(d) Others who come into contact with us.

5. What Information can we collect?

5.1. Generally, when anyone interacts with us here at OneLaw, we may collect and hold information that we obtain. That information includes (but is not limited to) the following:

(a) Name.

(b) Address.

(c) Date of birth.

(d) Identification/photograph.

(e) Contact details.

(f) Occupation and organisation worked for or owned.

(g) Technology, system, software, hardware and other device information.

(h) Location information.

(i) Log information (e.g. IP address).

(j) Information about the clients of our clients.

(k) Any other information which assists us in conducting our business, meeting our legal obligations, and providing our services.

5.2. When applying for a position at OneLaw, a candidate may be asked to supply other relevant details, such as information contained in a CV, driver licence, passport, immigration status, vaccination against COVID-19 status etc. We may also gather information from third parties such as identified referees. This information will be used to determine suitability for our vacancy.

5.3. OneLaw will collect information from its clients relating to their employees and own clients; such as a law firm's own client database. This information shall always be carefully protected, kept fully secure and only used for the provision of the legal practice management services that our clients have requested. Our Data Protection Policy shall be strictly followed at all times.

6. How do we collect Information?

6.1. We will usually collect information through face-to-face and virtual interactions, interviews, telephone conversations, electronic communications, and data provided to us from our workers, clients and other third parties. We may also obtain information through our website www.onelaw.co.nz as well as via applications (such as OnePractice, OneDesktop, OneAuthor, OneCollect, and OneLaw Cloud), including through the use of 'cookies'.

6.2. Our website and applications may include links to other websites, for which we make no representations or warranties about and are not therefore responsible for.

6.3. We have a QR code that users of the COVID-19 Tracer App may be required to use to scan in when visiting our workplace. We understand that information of such App users will only be used by contact tracers for tracing purposes. For people who do not have the COVID-19 Tracer App, we also have physical non-QR records. In accordance with the guidance from the Office of the Privacy Commissioner, we will take steps to ensure such records are protected and private (subject to being used for contact tracing purposes).

7. How do we hold, use and disclose Information?

7.1. Under the Privacy Act 2020, we are all obligated to protect the security of the information that we have.

7.2. We shall only use and disclose information that we at OneLaw have for the primary purpose it is collected, for reasonably expected secondary purposes, and any other reason which the Privacy Act 2020 requires us to. Generally, this means that our use and disclosure of information is only to be:

(a) To carry out our business.

(b) To provide, market and enhance our legal practice management software services.

(c) To enable proper communication with our clients and other related people and entities.

(d) To meet our legal obligations.

7.3. All of us here at OneLaw shall all take necessary steps to securely protect the information we have from misuse, unauthorised access or alteration, and loss or modification. We will use tools such as restrictions on electronic access and physical security.

7.4. When we no longer require information for permitted purposes, and in accordance with the Privacy Act 2020, we will take reasonable steps to return or destroy it.

7.5. We may disclose information to:

(a) Companies or individuals who assist us in providing our legal practice management software services.

(b) Any other organisation who may require the information for us to meet our legal obligations.

(c) Anyone else who we are authorised to disclose it to.

7.6. We will, however, never sell information to another party, and will only share it with others when required to do so.

8. Privacy Breach Principles

8.1. Under the Privacy Act 2020, we are required to report a notifiable privacy breach to the Office of the Privacy Commissioner. A notifiable privacy breach includes unauthorised or accidental access to, or disclosure of, personal information, or an action that prevents us as an agency from accessing personal information on either a temporary or permanent basis, that causes (or is likely to cause) serious harm.

8.2. When considering whether there has been (or is likely to be) such serious harm, we will be guided by the factors set out in section 113 of the Privacy Act 2020. These include:

(a) Actions already taken to reduce the risk of harm.

(b) The sensitivity of the affected information.

(c) The nature of harm that may be caused.

(d) Whether the information is protected by security measures.

(e) The person or body that has (or may have) obtained the information.

(f) Any other relevant matters.

8.3. We have already taken steps to mitigate the risk of a privacy breach, and will continue to do so. In particular, we have strong cybersecurity protections, clear directions as to security of information, and clear notification plans. All our workers must strictly continue to follow our directions in relation to mitigation of such risks and notifiable breaches at all times.

8.4. If any of our workers are concerned that there has been or may have been a privacy breach, they are to notify our Privacy Officer immediately. We will then undertake the assessment of serious harm referred to above. If, having undertaken this assessment, it is determined that the privacy breach has or is likely to cause serious harm, we will notify the Office of the Privacy Commissioner and the affected individuals as soon as practicable and no later than within 72 hours.

8.5. We will document the serious harm assessment and decision-making process by using and maintaining the internal OneLaw breach register contained in Schedule 1 to this Policy. Our Privacy Officer, or alternatively their delegate, will use the internal breach register to:

(a) Assist with identification and management of any breach.

(b) Confirm a serious harm assessment has been undertaken.

(c) Document the reasons why a particular breach does or does not amount to a notifiable privacy breach for the purposes of the Privacy Act 2020.

(d) Confirm notification of any notifiable privacy breaches.

9. Access and Correction of Information

9.1. Our workers are entitled to request access to information that we hold about them and, if necessary, request correction of that information. Any such request should be in writing and made to our Privacy Officer. Our Privacy Officer will endeavour to respond to the request within 20 working days.

10. Review of this Policy

10.1. This policy shall be reviewed every two years, but may be reviewed at our discretion prior to this time period. Any review will endeavour to reflect any changes in law, technology and our operations. The most current version of this policy can be obtained from our Privacy Officer.

Policy Version: 1
Policy Date: February 2022

Schedule 1

Internal privacy breach register

Part 1: Identify and record the potential breach
What is the nature of the potential breach?
When did the potential breach occur?
How did the breach occur, who is affected, and how are they affected?

Part 2: Consider whether there has been (or is likely to be) serious harm
Who (person or body) has (or may have) obtained the information? [name/s]
How sensitive is the affected data? Rate on a scale from [1] to [5] (1 being not serious, 5 being extremely serious)
Is the information protected by security measures? [Yes] or [No]
What is the nature and severity of the harm that may be caused? E.g. personal, reputational etc.
What action has been taken already to reduce the risk of harm? What action will now be immediately necessary to reduce the risk of harm? E.g. immediately contacting the impacted parties, requiring that the relevant disclosed information be returned and/or deleted.

Part 3: Determine whether the breach amounts to a notifiable privacy breach based on criteria in the Privacy Act 2020 and as summarised in this Policy, and action to be taken
If [yes] the OPC and affected individuals must be notified as soon as practicable and no later than within 72 hours, and then decide what further action is needed
If [no] the affected individuals must be notified within 72 hours, and then decide what further action is needed
Record the further action taken and what review of the situation occurs

Part 4: Assessment Confirmation			
Completed by: [name/s]	**Date completed:** [date]	**Checked by:** [name/s]	**Date:** [date]