DATA PROTECTION POLICY

Table of Contents

1. Introduction

1.1. This Data Protection Policy applies to data and information provided to OneLaw by its employees, contractors, leadership, clients, suppliers and other external third parties that OneLaw interacts with. That includes the data and information provided to us so that 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.

1.2. We respect and value all data and information shared with us and will protect it.

2. Purpose

2.1. This Policy provides guidance on how OneLaw and its workers and leadership will comply with the requirements of the Privacy Act 2020 and the data protection requirements in our commercial client contracts. Such data includes (but is not limited to):

(a) Client (potential or actual) data and other information. This includes data and information relating to the clients of our OneLaw legal clients.

(b) Information relating to our workers and leadership.

(c) Internal business, strategic, pricing, technical and operational data, policies and processes.

(d) Data held in any form, including paper, electronic, software, and other forms.

2.2. We refer to all such data and information as **data** in this Policy.

3. Policy

3.1. OneLaw collects client data in order to properly design and implement our easy to use legal practice management software and to run our business. We are all aware that this data must be securely protected, and we are all to be committed to ensuring that it does not fall into the hands of a party who has no right to access that information.

3.2. This Policy is relevant to all aspects of data protection, including when we collect and use data, when it is given to another person or organisation in connection with the provision of our services, and when any information we hold is disposed of.

3.3. Data protection is a key responsibility of all of our workers (whether director, employee or contractor) at OneLaw. That responsibility must be taken seriously by all of us. It is easy to unintentionally disclose protected data to others. However, unless there are lawful means to do so or an exception is met, such a disclosure will be a breach of this Policy and a worker's general obligations to OneLaw.

3.4. As also stated in our Privacy Policy, we at OneLaw may only use and disclose data we are given for the primary purpose that it is collected, for reasonably expected secondary reasons, and for any other reason which the Privacy Act 2020 enables us to.

3.5. Generally, this means we will only collect, use, hold and disclose data for the following purposes:

(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.

4. Data Security

4.1. Data from our clients, workers, and our own business is to be stored securely, using quality security protocols. Our workers must strictly follow such protocols. Access to this data is protected and can only be accessed by our OneLaw workers who are authorised to do so. If it is necessary to use, or extract, any such data for use by another worker, the data must only be used appropriately and securely.

4.2. Client and worker data shall be kept only for as long as is necessary for us here at OneLaw to do our work and to comply with our legal and commercial obligations. Following that, it shall be deleted or securely destroyed in line with our Privacy Act and client obligations.

4.3. To ensure that unlawful or unjustified disclosure of the data we use and hold does not occur, our workers must avoid discussing any aspect of their work with us outside of OneLaw if that could result in one of our clients, or a particular individual, being identified and by doing so we would breach our commercial obligations to that client, or the individual's privacy.

4.4. When our workers leave their desks at the end of the day, or for a long period of time during the day, they should log out of our OneLaw IT infrastructure so as to avoid unauthorised access to our protected data.

4.5. OneLaw has a Privacy Officer who oversees data protection and all our workers and leadership shall follow their instructions relating to security of data.

5. Client Data

5.1. All client data must be handled entirely professionally and with the utmost security and care. All of us here at OneLaw are strictly required to always take all necessary steps to protect such data from misuse, unauthorised access or alteration, and loss or modification. We will use tools such as restrictions on electronic access and physical security.

5.2. Data which does not identify any client or individual may be used in an appropriate general way by OneLaw for statistical and reporting purposes. All requests for data not already made public by us need to be expressly approved by our Privacy Officer.

5.3. All physical client documentation shall be kept entirely confidential, protected, and can only be accessed by those workers that are authorised to have access to it. It must not under any circumstances be left lying around in public, unattended in vehicles, or at remote work locations.

6. Worker Data

6.1. Worker data shall be held by OneLaw to maintain proper employment and contractor processes and records, to comply with legislative requirements, and for our own lawful uses. This includes information required for salary records, leave entitlements, hours worked, remuneration and tax purposes, health and safety reasons, and to meet other legal obligations relating to work. Our Privacy Policy also provides examples of information that may be collected and used by us.

7. Email Protection

7.1. Data and privacy breaches represent a significant risk to our clients, stakeholders and the reputation of OneLaw. To limit the possibility of a data breach relating to the use of email, the following rules are to be followed at all times (in conjunction with other rules that we have):

(a) Our workers and leadership shall take all care when sending emails to ensure that the included content and information is accurate and relevant. This includes ensuring that

the recipient email address is correct, especially if the email contains client or personal data.

(b) When attaching documents to emails, the documents must be opened and checked by our senders before the emails are sent. This is to ensure that only the correct documents are attached and so that adequate data protection is always maintained.

(c) Only necessary information should be included in any email and its content is to be professional and appropriate.

(d) Emails to parties outside of OneLaw should be monitored particularly carefully.

(e) Workers must not open any email that looks like spam, having malware or is a fishing expedition. If they are unsure, they must check with our Chief Architect.

8. Security of Information at Work

8.1. It is vital that all technology and hardware used by OneLaw workers in their work is used correctly and securely. This includes (but is not limited to) computers, laptops, tablets, mobile phones, other devices and the applications and programmes on them (**Hardware**). If any such Hardware in a worker's possession is lost, stolen, or hacked (in any way), it must be reported immediately to our Privacy Officer.

8.2. All Hardware that is registered under one of our worker's names, shall be the responsibility of that worker.

8.3. No identifiable client data is to be kept unsecured on any Hardware. All Hardware must be either pin or password protected.

8.4. Workers must ensure their OneLaw system password is complex, and not easily accessible to others. We encourage a minimum of 10 characters for passwords that include both letters and at least one capital letter.

8.5. Workers must also not disclose their password to anyone. This includes individuals from within and outside OneLaw. The only exception to this is shared user accounts on our OneLaw IT infrastructure. If one of our workers fears that their password has been compromised, they must change it immediately and alert our Chief Architect.

8.6. All OneLaw computers run operating system and antivirus updates, which our workers must allow to run unimpeded. These updates often contain important security fixes and must be allowed, followed and applied for all Hardware.

8.7. Hardware provided to any worker by OneLaw must not be used by any other person (including dependents).

8.8. Personal online shared or other drives are not to be used by our workers to save or transfer files and other OneLaw work product or confidential data without prior permission from our Chief Architect.

9. Security of Data when Working Remotely

9.1. Sometimes our workers may work remotely (including from home). It is just as important that this Policy is strictly followed when working in this way.

9.2. If any of our workers accesses our OneLaw infrastructure at home, they must take the utmost care to ensure it is accessed safely, appropriately and legally. All care must be taken to ensure our data does not become compromised. Our infrastructure must be properly logged out of and not accessed by anyone who doesn't work for us.

10. Stored Financial Data

10.1. A client's financial data shall be used only for the purposes it was provided to us, and only held for as long as it is required to process payments and to meet other client and our internal financial requirements.

11. Personal Data Access and Correction

11.1. As stated in our Privacy Policy, all of us at OneLaw are entitled to request access to, and correct, personal information that is held about us. Access requests are to be made in writing to our Privacy Officer who will endeavour to respond within 20 working days.

12. Managing a Data Breach

12.1. Our Privacy Officer is responsible for managing the response to any data or privacy breaches. A data or privacy breach is the unauthorised access to or collection, use or disclosure of personal information. Any data or privacy breach is considered a serious matter.

12.2. All data and privacy breaches (actual or potential) must be reported to our Privacy Officer without delay, and the processes set out in our Privacy Policy shall be followed.

12.3. Any action in breach of this Policy (including contributing to a data or privacy breach) may be deemed to be a breach of the relevant employee's employment agreement or contractor's engagement and their obligations to OneLaw. It will likely be the subject of disciplinary action.

13. Review of this Policy

13.1. 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 and details of revisions can be obtained from our Privacy Officer.

Policy Version: 1
Policy Date: February 2022