

PRIVACY POLICY - AUSTRALIA

Effective Date: 9 October 2026

1. Introduction

The OR Company Pty Ltd trading as Aspen Surgical, (ABN 17082404760) at 4/47 Wangara Rd, Cheltenham, VIC, Australia, 3192 ("we", "us", "our") is committed to protecting privacy and handling personal information in accordance with the *Privacy Act 1988* (Cth) ("Privacy Act") and the Australian Privacy Principles (APPs), as amended from time to time including by the Privacy and Other Legislation Amendment Act 2024 (Cth). This Privacy Policy ("Privacy Policy") explains how and why we (or service providers on our behalf) collect, use, hold, and disclose your personal information.

We provide training and development services primarily to healthcare organisations, including hospitals, and understand the importance of maintaining the confidentiality of personal and health-related information.

2. Types of Personal Information We Collect

The kinds of personal information we collect and hold about you are the following types of personal information:

- Contact details such as name, email address and phone number
- Employment details such as role/title, department, organisation, medical speciality, and clinical interests
- Account details, such as username, password, account number, and other account details that are requested as part of the account setup and management process
- Communication details, such as communications, complaints, and enquiries you have submitted to us, including through email, calls, chat functionalities, forms, social media, or other means, and information you provide in response to quizzes, questionnaires, intake forms, and surveys
- Transactional details, such as transactions with us, method of payment, relevant billing and shipping addresses, payments received, transaction history, and other information relating to the products or services purchased by you or your employer
- Registration and training details such as registration for upcoming training sessions or classes, assessments, information relevant to training participation, and completion records.

We also collect and hold the following kinds of sensitive information about patients:

- Patient Age Group
- Patient Medical Condition
- Patient Gender.

We only collect sensitive information (including health information) where it is reasonably necessary for our services and with appropriate consent.

We also collect and hold information about how you access, use and interact with:

- Our website (<https://www.aspensurgical.com/>),
- Our application
- Our Learning Management System, and
- Our analytics and web tracking platform.

This information includes:

- Name
- Email address

- Enrolment details
- Course completion records
- Login data
- Device data, such as IP address, browser type, operating system, device type, device attributes, and language
- Usage data such as platforms used, pages viewed, form submitted, referring/exit pages, and information about how and when you use the website or platform
- Location data based on IP address.

3. How We Collect Personal Information

We generally collect your personal information directly from you whenever you interact with us, for example, when you register for training, purchase or use any of our products or services, communicate with or contact us, or otherwise visit our website, application, or our learning management system.

We also collect your personal information as follows:

- From your employer, namely hospital/employer clients who engage our services
- Through learning platforms (e.g. Learn wise)
- Automatically via website technologies (cookies and analytics).

We collect your sensitive information as follows:

- From a hospital in connection with a root cause investigation into a customer complaint.

4. Anonymity

Individuals have the option to interact with Aspen anonymously or using a pseudonym, where reasonably possible. For example, if you contact our enquiries line with a general question, you will not be asked for your name unless it is required to adequately handle your enquiry.

However, for most of your interactions with Aspen, your name, contact information, employer and enough information about the particular matter will be required to enable Aspen to deal with the matter fairly and efficiently. For example, if you enquire about training registration, we will require your name, contact information, employer, and registration information.

5. Purposes for Collection, Holding, and Use of Information

We collect, hold, and use your personal information so that we can provide our goods and/or services, administer our organisation and comply with the law. The specific purposes for which we handle your personal information are to:

- Make our Services, including delivering workplace training programs, available to you
- Manage our relationship with you and your employer, including entering into and fulfilling any transactions with you
- Authenticate your credentials or facilitate any login to our Services
- Register you for an account with our Services
- Manage and analyse enrolments, attendance, and certifications through our Services
- Report training outcomes to your employer or relevant organisation
- Support compliance, accreditation, and workforce capability requirements
- Improve our Services and user experience, including by analysing market and user trends and developing product or profile insights

- Manage customer service issues, including issues relating to the performance of our Services and customer feedback
- Notify you about changes to our Services or material changes to this Policy
- Supply medical devices, related products and associated services to customers
- Establish, administer and maintain customer accounts within our inventory management, ordering and customer management systems
- Process and assess credit applications for the provision of goods and services on credit terms
- Manage orders, deliveries, invoicing, payments and account administration
- Verify the identity and authority of customer representatives and authorised users
- Provide technical assistance and respond to product or service enquiries
- Maintain the security, integrity and operation of our systems, networks and services
- Manage customer feedback, complaints, quality assurance activities and product-related enquiries
- Establish, exercise or defend legal rights and claims
- To enable functionalities on our website and Services
- Analyse usage of our website and platforms
- Comply with legal and regulatory obligations and assist government and law enforcement agencies or regulators.

For customer account establishment and credit applications, we collect personal information necessary to verify authorised representatives, establish trading accounts, assess creditworthiness, and manage payment for goods and services provided.

We do not use personal information for unrelated purposes without consent.

6. Disclosure of Personal Information

We disclose personal information that you provide us or which we collect and hold to:

- Your employer (hospital or healthcare organisation) for reporting and compliance purposes.
- Trusted service providers we use to facilitate our business operations and administer our Services, including (i) IT and system administration providers, (ii) data storage and server providers, (iii) web hosting providers, (iv) vendors to facilitate payments and payment processing, (v) LMS platforms, and (vi) transportation and shipping providers.
- Analytics vendors in order to understand our digital property traffic and usage patterns and optimise our digital properties.
- Our affiliates and related entities, investors, and operational partners.
- Financial institutions and payment processors that facilitate electronic payments, including invoice payment and service fee settlements from clients.
- Professional advisers, such as lawyers, accountants, and other similar advisors.
- Regulators or government bodies where required by law.

We may also disclose your personal information to:

- Buyers or other successors prior to or in the event of a merger, acquisition, divestiture, restructuring, reorganisation, dissolution, or other sale or transfer of some or all of our assets, whether as a going concern or as a part of bankruptcy, liquidation, or similar proceeding, where the information is among the assets being transferred.

- Regulatory and governmental authorities, law enforcement agencies, and courts, as necessary to comply with applicable laws and regulations, respond to a subpoena, search warrant, or other lawful request for information, or to otherwise protect our rights.

We take reasonable steps to ensure all third parties handle personal information securely and confidentially.

7. Data Security and Confidentiality

In accordance with APP 11 of the Privacy Act, as clarified by the Privacy and Other Legislation Amendment Act 2024 (Cth), we take reasonable steps to protect personal information from misuse, interference, loss, and unauthorised access, modification or disclosure. These steps include implementing technical and organisational measures appropriate to the sensitivity of the information held.

We store all information about you in computer systems and databases operated by either us or our external service providers.

Our technical and organisational measures include:

- Secure learning platforms and systems with access controls
- Encryption of personal information in transit and at rest
- Use of identity and access management technologies to restrict access to systems on which personal information is stored and processed
- Required staff training in privacy, confidentiality, and data handling obligations
- Requiring all staff to comply with internal information security policies
- Vendor-management measures, including security reviews, limiting access to business need, monitoring vendor access to systems and data, and appropriate contractual requirements
- Regular monitoring, auditing, and system security reviews
- Incident response procedures for data breaches.

We will also take reasonable steps to destroy or de-identify personal information once we no longer require it for the purposes for which it was collected or for any secondary purpose permitted under the APPs.

8. Overseas Disclosure

We are likely to disclose personal information to recipients located outside Australia. These include our parent company and related entities, and service providers that host, process or support our systems and services.

The countries in which these recipients are, or are likely to be, located are:

- **United States:** Our parent company and related entities in the United States may access or receive personal information to administer, secure and support our systems and services. We also use analytics and web tracking services that process and store personal information in the United States, including usage data, device information, and location data derived from your IP address.
- **Canada:** We use cloud hosting services provided by Amazon Web Services (AWS), and certain personal information is stored and processed on AWS infrastructure located in Canada.

If we begin to disclose personal information to recipients in other countries, we will update this Policy.

Before we disclose personal information to an overseas recipient, we take reasonable steps to ensure that the

recipient does not breach the Australian Privacy Principles in relation to that information. For example, we enter into contractual commitments that bind overseas recipients to privacy standards equivalent to the APPs.

9. Access and Correction

You have a right to request access to or correction of personal information we hold about you by contacting us using our contact details in Section 11. There are some circumstances where we may refuse your request to access or correct your personal information where permitted or required by the Privacy Act. If we refuse your request, we will notify you in writing of the reasons for the refusal. If you disagree with our decision, you may make a privacy complaint using the complaints procedure set out below in Section 10. If we are unable to correct your personal information, you may ask us to include a statement that you believe your personal information is inaccurate, out of date, irrelevant or misleading. There is no charge for requesting access to, or correction of, your personal information, but we may require you to meet our reasonable costs in providing you with access (such as photocopying costs or costs for time spent on collating large amounts of material). We will respond to your requests to access or correct personal information within a reasonable time, which is generally within 30 days of receiving your request.

10. Complaints

If you have concerns about how your personal information is handled, including in relation to your request for access or correction of your personal information, please contact us in the first instance using our contact details in Section 11. We take all privacy complaints seriously and will acknowledge and respond within 21 days.

Our complaints process:

- We will investigate your concern and, where possible, resolve it promptly and confidentially.
- If we cannot resolve your complaint to your satisfaction, we will explain our decision in writing.
- If you remain dissatisfied with the way in which we have handled a issues, you can make a complaint to the Office of the Australian Information Commissioner (OAIC) at www.oaic.gov.au.

11. Contact Us

The OR Company Pty Ltd trading as Aspen Surgical
Australia & New Zealand

- Address: 4/47 Wangara Rd Cheltenham, VIC, Australia, 3192
- Phone: +61 3 9413 5555
- Email: anz@aspensurgical.com

12. Updates to This Policy

We may update this Privacy Policy from time to time to reflect changes in our personal information handling or collection practices or in applicable law. The latest version, including its effective date, is available on our website or by contacting us at the contact details set above in Section 11. Where changes are material, we will take reasonable steps to notify affected individuals.