Waratah Hotel Group Privacy Policy

Review draft | Revised 29 October 2026
Entity: Waratah Management | Venue: Hotel Lismore

1. About this policy

This policy applies to personal information handled by Waratah Management, operating under the Waratah Hotel Group brand, in connection with Hotel Lismore, including its website, bookings, promotions and venue services. In this policy, "we", "us" and "our" refer to Waratah Management. This policy explains how we collect, hold, use and disclose personal information in providing these services.

It applies to personal information we handle in providing those services, including information handled on behalf of venue owners or operators. Where a venue operator or an independent provider handles your information in its own right, its identity and any additional privacy arrangements should be made clear in the relevant collection notice or service terms. The group name does not make every associated business the same legal entity.

We handle personal information in accordance with the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs), to the extent they apply to us. Personal information is information or an opinion about an identified, or reasonably identifiable, individual.

2. Information we collect and hold

The information we handle depends on your dealings with us. It may include:

- your name, contact details, date of birth and identity or age-verification information where reasonably necessary or legally required;
- reservation, accommodation, function and event details, guest requirements, transactions, purchases, payment-related information and communications with us;
- preferences, feedback, loyalty participation, promotion entries, marketing permissions and interaction history, including interests inferred from your dealings with us;
- CCTV footage, incident reports and other venue security records, and photographs or recordings taken in accordance with section 10;
- website and device information, such as IP addresses, cookie identifiers, browsing activity and interactions with digital communications; and
- job application details, CVs, qualifications, employment history, references and other information reasonably necessary for recruitment.

3. Sensitive information and your choices

Sensitive information includes health information, certain biometric information and information about matters such as racial or ethnic origin, religious beliefs or criminal history. We collect it only where reasonably necessary and with your consent, unless collection is otherwise permitted or required by law. Examples may include allergies, accessibility requirements or information relevant to an incident or medical emergency. We do not use sensitive information for direct marketing without your consent.

You may deal with us anonymously or using a pseudonym where lawful and practicable, such as for a general enquiry. Identification or other details may be necessary for a booking, accommodation, payment, age verification or a legal obligation. If necessary information is not provided, we may be unable to provide the relevant service.

4. How we collect personal information

We generally collect information directly from you when you make an enquiry or booking, attend or stay at a venue, place an order, complete a form, join a mailing list or loyalty programme, enter a promotion, give feedback, contact us, interact with our websites or social media, or apply for employment.

We may also receive information from someone arranging a booking or event for you, venue owners or operators, booking and ordering platforms, payment and technology providers, recruitment providers, referees, or other sources where collection is lawful and reasonably necessary. If you give us information about another person, please make them aware of this policy and obtain any permission needed to provide their information.

We provide additional notices where appropriate at or before collection, or as soon as practicable afterwards. These may explain the relevant entity, purpose, any legal requirement, likely disclosures and consequences of not supplying information. This policy does not replace those notices.

5. Why we use and disclose personal information

We collect, hold, use and disclose information as reasonably necessary to:

- respond to enquiries, manage bookings and events, provide hospitality and accommodation services, process payments and administer our relationship with you;
- understand guest needs, record preferences, improve services and analyse business performance, including through CRM systems and guest segmentation;
- administer loyalty programmes, promotions and competitions, and send marketing where permitted as explained in section 7;
- manage safety, incidents, complaints, insurance matters, suspected misconduct and security, and verify identity or age where necessary;
- assess employment applications and manage recruitment; and
- operate and administer our business, obtain professional advice, comply with applicable laws and respond to lawful regulatory or law-enforcement requests.

We otherwise use or disclose information for the purpose for which it was collected, a related purpose you would reasonably expect (directly related for sensitive information), with your consent, or as otherwise permitted or required by law. We do not treat publication of this policy as consent to unrelated uses or disclosures.

6. Who may receive personal information

Depending on the service and purpose, recipients may include the relevant venue owner or operator; authorised staff; related businesses where the disclosure is lawful and reasonably necessary; and providers of reservations, accommodation, ordering, payments, CRM, marketing, IT, data hosting, analytics, security, event or administrative services.

We may also disclose relevant information to our legal, accounting, audit, insurance and other professional advisers; regulators and law-enforcement agencies where permitted or required; or parties involved in a proposed business transaction, subject to appropriate confidentiality and privacy arrangements.

We take reasonable steps to limit disclosures to information needed for the relevant purpose and to establish appropriate handling arrangements with service providers. Information is not freely available to every venue or associated business simply because we share a group name. Marketing disclosures remain subject to section 7.

7. Direct marketing and your preferences

We may send offers, news and information about venues, events and services where we have the consent or other lawful basis required for the particular channel. Commercial email and SMS communications must comply with the Spam Act 2003 (Cth), including applicable consent, sender identification and unsubscribe requirements. Telephone marketing is subject to applicable Do Not Call Register and telemarketing requirements.

Making a booking, purchasing a meal or attending a venue does not, by itself, give us unrestricted permission to send marketing. Where we seek express consent, the sign-up wording should make clear whether it covers one venue or marketing across Waratah Hotel Group. We keep records of express consent and respect the scope of your permission and preferences.

You may unsubscribe using the facility in a marketing message or by contacting our Privacy Officer. Email and SMS unsubscribe requests are free and will be actioned within five working days. Those facilities remain functional for at least 30 days after the message is sent and do not require you to create an account, log in or provide additional personal information. Other direct marketing opt-outs are actioned within a reasonable period.

Where APP 7 applies, you may also ask us to stop using or disclosing information to facilitate another organisation's marketing, and ask where we obtained your information, subject to applicable exceptions. We do not treat this policy as permission to disclose your details to unrelated commercial partners for their own marketing.

An opt-out from marketing does not prevent essential service communications, such as a booking confirmation, payment receipt or safety notice. We distinguish these communications from promotional messages.

8. Websites, cookies, analytics and advertising

Our websites and digital services may use cookies, pixels and similar technologies to operate site features, remember preferences, measure usage and campaign performance, and support advertising or remarketing where permitted. Information may include IP addresses, device and browser details, cookie or advertising identifiers, pages visited, referral sources and actions taken.

These technologies can involve personal information, including where an identifier or browsing activity is linked to you by us or a provider. Depending on the tools used, information may be disclosed to analytics, advertising or social media providers and processed outside Australia. Relevant collection notices and website controls should explain the tools, purposes, usual recipients and available choices.

You can manage cookies through browser settings and use any privacy or advertising controls provided on the relevant site or platform. Blocking some technologies may affect site functionality. Browser controls may not prevent every form of tracking. We assess tracking tools before deployment and seek consent where required, including for the collection of sensitive information.

Our sites may link to independent third-party services. Their handling of information is governed by their own privacy policies. Where we disclose information to those services, our own privacy obligations continue to apply.

9. Overseas handling and disclosure

Some technology and service providers may process, store or access personal information outside Australia. Likely overseas recipient locations include Canada, the United States and the United Kingdom, depending on the providers used. Additional information about a particular service or provider can be requested from our Privacy Officer.

Before disclosing personal information overseas, we take reasonable steps required by APP 8 to ensure the recipient does not breach the APPs in relation to that information, unless a lawful exception applies. Those steps may include assessing the provider and its handling practices and using appropriate contractual protections. We review destination countries as provider arrangements change.

10. CCTV, identification and photography

Venues may use CCTV for safety, security, incident investigation and legal compliance. Where CCTV operates, notices should make this clear. Access is restricted to authorised people with a legitimate need, and relevant footage may be provided to regulators, police, insurers or advisers where lawful.

Where a venue scans identification or uses a biometric identification system, the relevant collection notice should explain the information collected, purpose, operator, recipients, retention arrangements and lawful basis. Age verification, keeping an ID copy and collecting biometric templates are different practices and must each be justified. We limit collection to what is reasonably necessary or legally required.

Biometric information used for automated verification or identification, and biometric templates, are sensitive information. Collection generally requires consent and reasonable necessity unless a specific legal exception applies. A general security purpose or entry sign does not, by itself, establish a lawful exception.

We may arrange photography or video at venues and events for event coverage and promotion. We provide appropriate notice and explain intended uses, which may include websites, social media and venue materials. Attendance alone is not treated as unrestricted consent to every recording or promotional use. Please tell the photographer or venue team if you do not wish to be featured, or contact us about an image already published.

For featured promotional photographs or recordings, we seek appropriate permission. Particular care is taken with images of children, including permission from a parent or guardian where appropriate. Requests to avoid or remove identifiable images are considered promptly, taking account of what we control and any legal obligations.

11. Holding, security and retention

We hold information electronically and, where necessary, in paper records. Electronic records may be held in systems operated by us or service providers. We take reasonable technical and organisational steps to protect information from misuse, interference, loss and unauthorised access, modification or disclosure.

Depending on the information and system, safeguards may include access restrictions, authentication, staff training, secure storage and disposal, provider oversight and incident-response procedures. No system is completely secure, and we do not guarantee absolute security.

We retain information for as long as reasonably necessary for the purpose for which it was collected, legitimate operational needs and applicable legal obligations. Retention depends on the type of record, including booking, financial, employment, incident, CCTV and identity records. We do not keep all information indefinitely or apply one retention period to every record.

Where information is no longer needed for a permitted purpose and we are not required to retain it, we take reasonable steps to destroy or de-identify it, including through appropriate provider arrangements. Legal holds and mandatory record-keeping obligations may require longer retention.

12. Data breaches

If a suspected data breach occurs, we take steps to contain it, assess the circumstances, reduce harm and review the response. Where the Notifiable Data Breaches scheme applies, we take all reasonable steps to complete the required assessment within 30 calendar days of becoming aware of grounds to suspect an eligible breach.

Where we have reasonable grounds to believe an eligible data breach has occurred, we notify the OAIC and affected individuals as soon as practicable, unless a lawful exception applies. Notices explain the breach and recommended protective steps. A notification obligation does not apply to every security incident.

13. Access to and correction of your information

You may request access to personal information we hold about you, or ask us to correct information that is inaccurate, out of date, incomplete, irrelevant or misleading. Please contact our Privacy Officer and provide enough detail to help us locate the records. We may take proportionate steps to verify identity and authority before releasing information.

We respond within a reasonable period, generally within 30 days. If a request is complex or needs more time, we explain the position and keep you informed. Access may be limited or refused where the law permits, including to protect another person's privacy.

We do not charge to make an access request. Where permitted, we may charge a reasonable, non-excessive fee for providing access, such as reasonable retrieval or copying costs, and explain any proposed fee in advance. We do not charge for making a correction request, correcting information or associating a statement with a record.

If we refuse access or correction, we provide written reasons to the extent required by law and explain available complaint mechanisms. If we refuse correction, you may ask us to associate a statement of the correction sought with the information. Where required, we take reasonable steps to notify other APP entities of a correction if you ask us to do so.

14. Privacy enquiries and complaints

Please contact our Privacy Officer if you have questions, wish to exercise a privacy right or want to complain about how we handle personal information. Include the relevant venue or service, a description of the concern and the outcome you are seeking.

We take complaints seriously and handle them as confidentially as practicable, sharing information only as needed to investigate, respond or comply with law. We aim to acknowledge complaints within seven days and resolve them within 30 days. If more time is needed, we explain why and provide an expected timeframe.

If you are dissatisfied with our response, or we have not responded within a reasonable period, you may complain to the Office of the Australian Information Commissioner (OAIC). Information about the OAIC's complaints process is available at www.oaic.gov.au/privacy/privacy-complaints or by calling 1300 363 992.

15. Contact details

Privacy Officer
Waratah Management
Waratah Hotel Group
Email: privacy@waratahmanagement.com.au
Telephone: (02) 9098 9100
Office: Suite 702, 116 Military Road, Neutral Bay NSW 2089
Postal: PO Box 605, Neutral Bay NSW 2089

Venue covered by this policy
Hotel Lismore
110 Woodlark Street, Lismore NSW 2480
Please direct privacy enquiries and complaints to the Privacy Officer using the contact details above.

16. Policy availability and changes

This policy is available free of charge on our websites. You may request a copy from our Privacy Officer, including in another accessible format, and we will take reasonable steps to accommodate your request.

We review this policy and our information-handling practices as our services, systems and legal obligations change. Updated versions will be made available on our websites with a revision date. Where required, we also provide updated collection notices or seek fresh consent; changing the policy does not itself authorise a new use or disclosure.