

Privacy Policy

Shockwave Media Pty Ltd · ABN 26 606 414 493 · Based in NSW, Australia

Version v1.0 Approved 8 October 2026 Effective 8 October 2026 Owner Managing Director
Next review October 2027

Document control

VERSION	DESCRIPTION	APPROVED BY	APPROVAL DATE	EFFECTIVE DATE
v1.0	Initial release	Daniel Hooper, Managing Director	8 October 2026	8 October 2026
Policy owner	Daniel Hooper, Managing Director			
Applies to	All personal information collected, held, used or disclosed by Shockwave Media Pty Ltd, including personal information we handle on behalf of government and other clients			
Review	Annually. Next review due October 2027, or earlier if law, contract requirements or our operations change materially.			
Published at	shockwavemedia.com.au/government/policies/			

01 About this policy

This policy explains how Shockwave Media Pty Ltd manages personal information in line with the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs). We apply the APPs to all personal information we handle. When we act as a contracted service provider to an Australian Government agency, we also comply with the privacy obligations in that contract. When we handle personal or health information for NSW public sector agencies, we comply with the Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act) and, where relevant, the Health Records and Information Privacy Act 2002 (NSW), as our contracts require. The Managing Director is our privacy officer and is accountable for this policy. All staff complete privacy training at induction and annually. Privacy complaints, access requests and breaches are recorded and reviewed at least annually.

02 What we collect and how

- ◆ **Clients and prospective clients:** names, roles, business contact details and correspondence.
- ◆ **Website visitors:** information submitted through our contact form (name, work email, organisation, topic, optional timeframe and message), and technical data such as IP address and browser type recorded in server logs. Our website sets no advertising or tracking cookies and loads no third-party scripts. To prevent spam, it keeps a one-way (hashed) form of the visitor's IP address to limit repeated submissions, and deletes it within 30 days of the last submission.

- ◆ **Job applicants, staff and contractors:** information needed for recruitment and employment, including employment history, references and, where required, background checks.
- ◆ **Suppliers:** contact and payment details.
- ◆ **Client data:** personal information contained in systems we build, host or support for clients.

We collect personal information directly from the person where practicable, and only where it is reasonably necessary for our functions and activities. We do not collect sensitive information unless the person consents, or the law or a client contract permits it. You can deal with us anonymously or under a pseudonym where that is practicable.

03 Use and disclosure

We use personal information to provide and improve our services, respond to enquiries, manage client and supplier relationships, recruit and manage staff, meet legal obligations and keep our systems secure. We disclose it only for those purposes or with consent, including to service providers who support our business (such as cloud hosting and software tools) under confidentiality and security obligations, or where required or authorised by law. We do not sell personal information. We send marketing only where permitted and every message includes a way to opt out.

Client data: we handle personal information in client systems only on the client's instructions and for the purposes of the engagement. We do not use client data, including government data, for any purpose of our own, including training AI models for ourselves or other clients. We train or fine-tune a model on a client's data only when that client engages us to, and only for that client. The client remains responsible for its own privacy obligations to the individuals concerned.

04 Data held in Australia and overseas disclosure

For NSW and Australian Government engagements, the client systems and data we build, host or support, including backups, are hosted in Australia, and the work is delivered by Australian-based staff. We do not store or process that data outside Australia unless the client agrees in writing. We handle client data in line with Australian regulations, and data relating to Australians is kept on Australian servers. Our business email runs on Google Workspace, whose data centres may be located outside Australia.

05 Security and retention

We protect personal information with the controls in our Information Security Policy, including access control, multi-factor authentication, encryption, logging and staff training. We destroy or de-identify personal information when it is no longer needed, subject to legal and contractual retention requirements. We keep enquiry emails for up to 2 years and server logs for up to 90 days, then delete them. At the end of a client engagement, we return or destroy client data as the contract requires.

06 Data breaches

We assess suspected data breaches promptly and in any case within 30 days. Where a breach is an eligible data breach under the Notifiable Data Breaches scheme, we notify affected individuals and the Office of the Australian Information Commissioner (OAIC). Where a breach involves client data, we notify the client within 24 hours of becoming aware of it, or sooner if the contract requires, so that it can meet its own obligations, including a NSW agency's obligations under the Mandatory Notification of Data Breach scheme in the PPIP Act.

07 Automated decisions

We do not use personal information to make automated decisions that significantly affect individuals' rights or interests in our own business. Where we build AI or automation for clients, we support the client to meet its own transparency obligations.

08 Access and correction

You can ask to access or correct personal information we hold about you via the contact form at shockwavemedia.com.au. We will verify your identity and respond within 30 days. If we refuse, we will give reasons in writing and tell you how to complain. If the information is held for a client, we will refer the request to that client and help them respond.

09 Complaints

Please raise privacy complaints via the contact form at shockwavemedia.com.au. The Managing Director will acknowledge complaints within 5 business days and aim to resolve them within 30 days. If you are not satisfied, you can complain to the OAIC (oaic.gov.au). Where the complaint concerns information we handle for a NSW public sector agency, you can also contact that agency or the NSW Information and Privacy Commission (ipc.nsw.gov.au).

10 Review

This policy is reviewed annually and when privacy law changes. Based in NSW, Australia. Contact us via shockwavemedia.com.au.

Approval

Approved by Daniel Hooper, Managing Director, Shockwave Media Pty Ltd.

Approval date: 8 October 2026 · **Effective date:** 8 October 2026 · **Next review:** October 2027

Signed: Daniel Hooper (signed original held on file)