



LEGAL POLICY

Privacy Policy

1.4

How we collect, use, and protect your personal information.

DATE

27 August 2026

ABN

74 101 234 664

Real World Technology Solutions · rwts.com.au

About this Policy

This privacy policy explains how Real World Technology Solutions and its related entities collect, use, disclose and store your personal information. In this policy, 'we', 'us' and 'our' refer to:

- Real World Technology Solutions Pty Ltd (including its Red Globe Productions and Lux Imperium brands)
- Real World Networks Pty Ltd
- Blueteq Pty Ltd
- Industrious Partners Pty Ltd
- and any other subsidiary or related entity.

If anything here isn't clear, please email us at privacy@rwts.com.au.

Our Principles

We have a simple approach to data protection and privacy which adheres to the **Australian Privacy Principles** (APPs).

Our obligations under the Privacy Act 1988 (Privacy Act):

- This privacy policy sets out how we comply with our obligations under the Privacy Act. As an Australian-based organisation, we are bound by the APPs in the Privacy Act, which regulate how organisations may collect, use, disclose and store personal information, and how individuals may access and correct personal information held about them.
- In this privacy policy, 'personal information' has the same meaning as defined by the Privacy Act: information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

We also operate within the broader privacy framework that applies in Australia, including the protections introduced by the Privacy and Other Legislation Amendment Act 2024.

Collection

We collect your personal information so that we can provide you with the products, services or information that we supply. Sometimes we collect personal information from a third party or from a publicly available source, but only if you have consented to your information being used in this way, or would reasonably expect us to collect it in this way. We only collect this information from companies or sources that are allowed to disclose it to us. Below you'll find a breakdown of the different ways your personal information is collected.

What we collect from you

Contact and enquiry forms When you complete a contact or enquiry form, we collect the details you provide (such as your name, email, phone number and message) and use them to respond to you. If your

enquiry relates to our services, we may follow up with relevant information in line with what you originally asked about.

Payments If you make a card payment with us directly, your card details may be handled by us only for as long as it takes to process the payment, after which they are securely destroyed. Where you pay through a third-party payment provider, we receive only basic confirmation of payment — your card details are handled by that provider under their own terms and privacy policy.

Mailing lists If you opt in to one of our mailing lists, you consent to us emailing you about what we do as a company. We won't spam you. We send these in line with the guidelines set out by the Australian Communications and Media Authority, and every message includes an unsubscribe option. You can read more in the Direct Marketing section below.

Support requests If you contact us for technical, product or account support, we may keep a record of that interaction — including transcripts, emails and the details you share — through our support platform, so we can resolve your request, for training purposes, and to improve our service. Some support work is assisted by the tools described in the Service Providers and AI Tools section below.

Accounts and logins If you create an account with us using your personal details, we collect that information so your preferences are stored and available when you return and log in.

Information we collect automatically When you use our websites, we and our service providers collect certain technical information automatically, including your IP address, browser and device type, pages visited, and similar diagnostic data. We use cookies and similar digital identifiers for the following purposes:

- **Site performance:** to keep the site secure and working, and to understand how it's used so we can make improvements.
- **Analytics:** to understand visitor numbers, which areas of the site are popular, and which areas we need to work on.
- **Security and anti-abuse:** to protect our sites from automated abuse, spam and fraud (for example, using Cloudflare and hCaptcha — see below).

Cookie rights: You can always disable cookies by changing the settings of your browser. Just bear in mind this may affect how some items on our website are displayed.

Information from third parties We may receive personal information from third parties where you've consented or would reasonably expect it — for example, if you contact us through a social or professional platform, where a partner refers you to us, or from publicly available sources. Any information collected directly by those platforms is governed by their own privacy policies.

Embedded content Some of our pages include embedded content (such as maps or videos) hosted by third parties. That content is not hosted on our servers, and any interaction with it is governed by the relevant provider's privacy policy, not ours.

Information we collect in providing telecommunications services

When we provide telecommunications services, we may collect more detailed information, including:

- **Financial and credit information** related to your financial relationship with us, such as your income details, payment history, credit history and service history. For more details, see the Credit Reporting section below.
- **Information about your products and services**, such as device-specific information including your hardware model, operating system version, unique device and service identifiers, device status, serial numbers, settings, configuration, and software and mobile network information.
- **Information about how you use your products and services**, such as:
 - your network usage, including the time and duration of your communications, and information about the operation of the equipment, services and applications you use on our networks;
 - how you use our services to access the internet, such as information about websites visited;
 - your location or the location of your devices when you are using our products and services; and
 - information that allows us to identify you for verification purposes, including, where you have given us permission to do so, biometric information such as your fingerprints and voice patterns. (Document Verification Service checks, described below, involve no biometric information).
- **Technical information about your products and services**, including details about our network performance and how you use our networks.

We handle this information in accordance with the Privacy Act and the telecommunications-specific privacy obligations that apply to us, including under the Telecommunications Act 1997.

Sensitive information

Sensitive information includes information about a person's race, ethnic origin, political opinions, health, religious or philosophical beliefs and criminal history. We may collect some forms of sensitive information. For example, we may collect limited health information to provide priority assistance services, or a Centrelink customer reference number to provide a pensioner discount. We are subject to strict requirements in relation to sensitive information, including to only collect and use it with consent or otherwise in accordance with applicable law such as the Privacy Act 1988 (Cth).

Identity Verification and the Document Verification Service

Before we can connect a telecommunications service, we need to be confident you are who you say you are. To do that, we use the Australian Government's Document Verification Service (DVS).

How we use the DVS. When you apply for a service, we ask you for details from an identity document — an Australian driver licence, passport or Medicare card. With your consent, we send those details to the DVS, which checks them against the records held by the agency that issued the document. The DVS returns a simple match or no-match answer. It does not send us any new information about you, and the DVS itself does not store your details. We connect to the DVS through RapidID, an approved Gateway Service Provider.

How the Attorney-General's Department handles your information. The DVS is operated by the Attorney-General's Department. Its role is to pass the details you give us to the agency that issued your document

and to pass the answer back — the DVS does not keep any of it, and the department cannot see or change what passes through. The department engages a service provider to run the DVS, bound by the Australian Privacy Principles and strict security standards, and publishes its own **Privacy Statement — Identity Verification Services** explaining how it handles personal information.

If your document lists other people. Some documents — a Medicare card, most often — list other people as well as you. If you give us a document like that, we take it that you have told those people and have their consent. Their details are used only to verify your document, and we handle them the same way we handle yours.

What we're required to do. As a carriage service provider we have to verify the identity of our customers before we supply certain services, under the Telecommunications Consumer Protections Code and the ACMA's customer identity authentication rules. Our use of the DVS is governed by the Identity Verification Services Act 2023 (Cth), our Participation Agreement with the Attorney-General's Department, and the DVS Access Policy. Everything we collect for this purpose is personal information under the Privacy Act 1988 (Cth) and is handled in line with this policy.

What we keep, and what we don't. We don't retain your identity document numbers, and we don't keep copies or photographs of your identity documents. Where you supply a document to us directly rather than through our online process, we securely destroy it once the verification is complete. What stays on your customer record is your name, date of birth and address, along with a record of the verification transaction — the date, the reference number and whether the check matched. We keep that transaction record so we can demonstrate that we met our obligations if we're ever asked.

What we never do with it. We never use identity information to build a profile of you, to market or advertise goods and services to you (or let anyone else do so), or for market research. Our agreement with the Attorney-General's Department prohibits it.

Overseas disclosure and verification assistance. We do not send your identity information to overseas recipients. In the rare case that we ask the Attorney-General's Department for help verifying a document, the department collects your information for that purpose and handles it under the Privacy Act 1988 (Cth) and its own privacy statement.

Your rights. Giving consent is your choice. You can ask us what we hold about you and ask us to correct it, and you can make a complaint if you think we've handled your information poorly. Those rights are set out in the Access and Correction and Complaints Handling sections below and apply to identity verification the same as anything else.

If you'd rather not consent. You don't have to use the DVS. Tell us and we'll verify your identity another way — in person at our office, or through another arrangement we work out with you. It usually takes longer, and we may need to see more than one document, but it won't stop you becoming a customer. What we can't do is supply the service without verifying your identity at all, because we're required to do it.

If something goes wrong. If you have a concern about how your information was collected, used or disclosed through the DVS, contact us first at privacy@rwts.com.au or on 1300 798 718 and we'll work through it with you. If you're not satisfied, you can take it to the Office of the Australian Information Commissioner (oaic.gov.au, 1300 363 992) or, for telecommunications matters, the Telecommunications

Industry Ombudsman (tio.com.au, 1800 062 058). You can also read about the identity verification services and how to raise concerns about them at idmatch.gov.au.

If you need this information in another format — large print, or talked through over the phone — call us on 1300 798 718 or email privacy@rwts.com.au and we'll arrange it.

Information about other people

You might also need to provide personal information about other individuals to us (for example, about your authorised representative). If so, we rely on you to have informed those individuals that you are giving their personal information to us, and to have advised them about this statement.

It is important to be aware that if you access another party's website or application using one of our products, that other party will deal with your personal information in accordance with its own privacy policy.

Use and Disclosure

We only use personal information for the purpose for which it was provided, or for purposes that directly relate to one of our functions or activities. We will not provide your personal information to other entities, bodies or any other party unless one of the following applies (consistent with APP 6 — use and disclosure of personal information):

- You have consented.
- You would reasonably expect, or have been informed, that information of such kind would be passed on to those individuals, entities or bodies.
- It is otherwise required or authorised by law, or reasonably necessary for the enforcement of a criminal law or of a law imposing a pecuniary penalty, or for the protection of public revenue.
- It may prevent or lessen a serious and imminent threat to somebody's life or health.

Service Providers and AI Tools

To run our business and deliver our services, we use trusted third-party providers who process information on our behalf. We choose providers that maintain strong security and contractual protections, and we only share what's necessary for them to do their job.

Infrastructure and hosting. Our systems and websites run on cloud and infrastructure platforms including Amazon Web Services, Microsoft Azure and Google Cloud. We use Cloudflare for content delivery, network security and protection against attacks, and hCaptcha to protect our forms from automated abuse.

Productivity and communications. We use business platforms such as Microsoft 365 and Google Workspace, and associated tools, to operate day to day. We use Zendesk to manage and respond to support requests, and HubSpot as our customer relationship management and marketing platform.

Identity verification. We use RapidID, an approved Gateway Service Provider for the Australian Government's Document Verification Service, to verify identity documents when you apply for a service. See Identity Verification and the Document Verification Service above.

Managed services tools. To deliver and support our managed IT services, we use remote monitoring and management, professional services automation, and backup and business continuity tools provided by Kaseya, including Datto. These tools help us monitor, manage, support, secure and back up the systems and devices we look after for our managed services customers, and in doing so may process information held on or about those systems.

Security tools. We use endpoint protection, detection and response, and antivirus tools — including Huntress and Bitdefender — to protect the systems and devices we manage against threats. These tools process security-related information about those systems, which may include limited personal information, to detect, investigate and respond to security threats.

Payments and receivables. We use Marmalade Australia Pty Ltd to issue and reconcile invoice payments, and we may assign individual invoices to Marmalade. Marmalade may collect credit information about our customers from credit reporting bodies for its own assessment purposes, and may hold or access information outside Australia, including in New Zealand, the United States, Singapore and countries in the European Union.

Credit and business information. We use commercial credit and business information providers, including CreditorWatch, to check the creditworthiness of business customers, and we deal with a trade credit insurer and its broker in connection with insuring amounts owed to us. Our Credit Reporting Policy has more detail about these arrangements.

We also engage other reputable providers from time to time to deliver and support our services. We hold these providers to appropriate security and confidentiality obligations, and only share what's necessary for them to do their job.

Artificial intelligence tools. We use AI tools — including services from Anthropic (Claude), OpenAI (ChatGPT) and Microsoft (Copilot) — to help us work more efficiently. This includes diagnosing problems and developing solutions, analysing data and reviewing details, drafting documentation, generating scripts and code, and assisting with support queries. AI augments our team's work; it does not replace the people who review and act on the outputs.

When we use AI tools in connection with customer-related work, we do so under enterprise or business agreements that include important safeguards for your data:

- **No model training:** information we share with these tools is not used to train or improve the underlying AI models.
- **Data retention limits:** these services are configured to retain data only for the minimum period needed to provide the service, typically deleted within 30 days or less.
- **Access controls:** only authorised team members can use these tools, and usage is subject to our internal policies and general supervision.
- **Output review:** we review AI-generated outputs before acting on them or sharing them with you, and redact any sensitive information that should not be included.

Some of our AI-assisted processes are partly automated, which means your information (including attachments or support details) may be processed by these tools as part of delivering our services. The enterprise agreements we have in place ensure this data remains protected and is not retained or used

beyond the immediate task. A member of our team remains responsible for the decisions that affect you — these tools assist that work rather than making final decisions about you on their own.

Overseas disclosure. Several of the providers above store or process information outside Australia, including in New Zealand, the United States, Singapore and countries in the European Union. Where we disclose personal information overseas, we take reasonable steps to ensure it is handled consistently with the Australian Privacy Principles, including through the contractual protections in our agreements with these providers.

We treat AI tools as we would any other third-party service provider. The same care we apply to protecting your information with other suppliers applies here.

Opt-out: If you would prefer your information not be processed using AI tools, please let us know at privacy@rwts.com.au and we will make arrangements to accommodate this where possible.

Automated Decision-Making

We do not use computer programs to make decisions that have a significant effect on you without meaningful human involvement. Where we use automated or AI-assisted tools to support our work — for example, to help triage support requests or process administrative information — a member of our team reviews the relevant outputs and remains responsible for any decision that affects you. If this changes, we will update this policy to explain what information is used and what kinds of decisions are involved, in line with our obligations under the Privacy Act.

Direct Marketing

When it comes to direct marketing, no one likes being spammed. At Real World Technology Solutions, we may use your personal information to send you advertising that is customised to your interests, characteristics or general location.

Opt-out: As with all direct marketing correspondence you receive from us by email, there is always an unsubscribe button or link at the bottom of the email. With this you can manage which messages you receive from us.

Quality of Personal Information

We do what we can to keep your personal information up to date and accurate at all times, as this allows us to deliver a better service to you. If any information we hold for you needs to be corrected, you can contact us at privacy@rwts.com.au.

Data Security

We take active steps to protect the personal information we hold against loss, unauthorised access, use, modification or disclosure, and against other misuse. These steps include password protection and access controls for our IT systems, as well as technical and organisational measures appropriate to the information we hold. While we cannot share details of our entire security system for safety reasons, you can always contact us at privacy@rwts.com.au with any questions.

When no longer required, or when requested by you, personal information is destroyed or de-identified in a secure manner.

If we become aware of a data breach that is likely to result in serious harm to individuals whose personal information we hold, we will assess it and notify affected individuals and the Office of the Australian Information Commissioner as required under the Notifiable Data Breaches scheme.

Access and Correction

At Real World Technology Solutions, we do everything we can to keep your personal information accurate. If you find that any information we hold about you is incorrect, you can contact us at privacy@rwts.com.au, or via the contact details below, and we will endeavour to assist you. Please bear in mind that under Australian privacy laws, there may be situations where we cannot provide access to such personal information — for instance, if doing so would reasonably affect someone else's privacy, or may pose a threat to someone's life, health or safety.

For any personal information collected by third parties, even when you are visiting our website, it is best to view their privacy policy and seek assistance from those parties directly.

Credit Reporting

Our [Credit Reporting Policy](#) sets out in full how we collect, hold, use and disclose credit information and credit eligibility information about individuals, including our dealings with credit reporting bodies. The following is a summary.

Sometimes, such as when we are checking your credit worthiness or assessing your credit situation, we might collect credit information from, or give information to, credit reporting bodies. Credit information can include:

- identification information;
- details about information requests made about you to credit reporting bodies;
- current and historical details about credit applications you have made and credit arrangements you have entered into;
- information about overdue payments, default listings, serious credit infringements, and information about payments or subsequent arrangements in relation to either of these;
- various publicly available information such as bankruptcy and credit-related court judgments; and
- credit scores or risk assessments indicating an assessment of your credit worthiness.

Credit information relates primarily to your dealings with other credit providers (for example, banks, other financial institutions, or other organisations that may provide you with credit in connection with their products or services). It may also include certain credit worthiness information that we derive from the data we receive from a credit reporting body. Sometimes we may collect this information about you from other credit providers.

We may disclose your credit information to credit reporting bodies. They in turn may include it in credit reporting information they provide to other credit providers to assist them to assess your credit worthiness.

We may use or disclose your credit information for purposes such as:

- developing our credit assessment and credit worthiness rating system;
- processing credit-related applications and managing credit that we provide;
- assisting you to avoid defaults;
- collecting amounts you may owe us in relation to such credit, and dealing with serious credit infringements;
- assigning our debts, or acting in connection with any securitisation or other financing arrangement;
- participating in the credit reporting system;
- dealing with complaints or regulatory matters relating to credit or credit reporting;
- when required or authorised by another law; and
- the purposes set out in the Collection and Use and Disclosure sections above, except in relation to information we collect from credit reporting bodies.

You have the right to request credit reporting bodies not to:

- use your credit eligibility information to determine your eligibility to receive direct marketing from credit providers; and
- use or disclose your credit eligibility information if you have been, or are likely to be, a victim of fraud.

Complaints Handling

If you have any complaints, or feel that there has been a breach of the Australian Privacy Principles or a registered APP code, you can contact us at privacy@rwts.com.au or via another option below.

If you are not satisfied with the process of making a complaint to our Privacy Officer, you may make a complaint to the Information Commissioner using the details below:

Office of the Australian Information Commissioner GPO Box 5218 Sydney NSW 2001 Email:
enquiries@oaic.gov.au Telephone: 1300 363 992

How to Contact Us

We understand that your personal information is important to you, and we're glad you made it this far. If you have any questions or concerns about this policy or our practices, you can get in touch with us in the following ways:

Email: privacy@rwts.com.au Address: Real World Technology Solutions, PO Box 1385, Macquarie Centre PO, North Ryde NSW 2113