



Privacy Notice

Effective date: 3 February 2026

1. Introduction

This Privacy Notice explains how The Messaging Company Pty Ltd (ACN 669 674 382), its related entities, and its local agents and/or associates (together “**we**”, “**our**” or “**us**”) collect, use, store, share, and safeguard personal data. It also outlines the rights you have in relation to your personal data, including how you can access, rectify, or update the information we hold about you, in accordance with applicable data protection and privacy laws.

2. Personal data we collect

In this Privacy Notice, we use the term “**personal data**”. When we use this term, we mean information that can identify or be linked to you as an individual.

We collect different types of personal data depending on how you interact with us. This includes information you provide directly, information collected automatically through your use of our services, and information obtained from third parties.

Information you provide directly

We collect personal data that you choose to provide to us, for example when you create an account, communicate with us, or purchase our products or services. This may include:

- identifying information such as your full name, job title, employer or organisation, and gender;
- account information, including your username;
- contact details such as your residential, office, and billing addresses, telephone and mobile phone numbers, and email addresses;
- purchase and transaction information, including details about payment methods and payments to and from you, and other details of services and products you have purchased from us;
- marketing preferences, including your choices about receiving marketing communications from us;
- records of our interactions and correspondence with you via phone, when submitting a web form or online chat interaction, email, text message, social media, or otherwise;

- customer service information, including your customer service enquiries and comments, feedback, and survey responses;
- information required to meet our legal obligations (e.g. data relating to contracts, payments, and communications sent or received via our services); and
- a copy of any email reported as misclassified (e.g. spam, not spam, phishing, malware, etc.).

Information collected automatically

When you use our websites, mobile applications, or online services, we automatically collect certain information about your device and activity. This may include:

- usage data about how you interact with our services;
- location data, including both physical and virtual locations (e.g. IP addresses);
- information collected from cookies, beacons, tags, and scripts, including details about your interaction with our online presences, such as the pages you visit, the number of visits, the number of scrolls, language preferences, webpage interactions and searches, IP address, and the location of the devices accessing our websites and services, demographic information about you, your user settings, and analytics data; and
- log file information automatically reported by your internet browser or mobile application each time you access our websites or services, including information such as your operating system, device type, unique identification number, browser type, geographic location, referring/exit pages and URLs, number of clicks, domain names, landing pages, pages viewed.

3. Information obtained from third parties or linked accounts

We may also receive information about you from third parties, including when you link or integrate third-party services with your account. This may include:

- information about any third-party accounts you connect or link to your account with us;
- technical information or metadata received through linked accounts or services (e.g. to retrieve or send emails, or to attach/save files); and
- verification or anti-fraud data obtained from payment processors or compliance partners where required by law.

The above list is not exhaustive and in specific instances we may need to collect additional personal data for the purposes set out in this Privacy Notice.

If you do not provide the personal data we require to deliver our products or services, we may be unable to provide certain features or services to you.

4. How we use your personal data

The table below explains the purposes for which we use your personal data and the corresponding legal basis.

Purpose	Legal basis
To operate, maintain, and provide to you (or your service providers) the features and functionality of our websites, products, and services	Contract - processing is necessary for the performance of a contract with you
To process, manage, and deliver customer accounts	Contract
To provide you with quotations, updates, and information related to our services (including steps taken prior to entering into a contract)	Contract / Pre-contractual steps
To notify you about changes to our services, terms of service, or this Privacy Notice	Contract
To establish your identity and verify your account	Contract
To send you marketing communications (including newsletters or promotional materials)	Consent - where you have provided your consent, which you can withdraw at any time
To respond to your questions and concerns or to enable you to exercise your legal rights (such as data subject access requests)	Legal obligation
To comply with our legal obligations and other regulatory or compliance requirements	Legal obligation
To administer and protect our organisation, products, services, and websites, including troubleshooting, data analysis, testing, system maintenance, support, reporting, hosting, security, vulnerability and fraud detection, and protection activities	Legitimate interest - to ensure the effective and secure operation of our business and IT systems
To improve our websites, products, services, marketing, customer relationships, and user experiences (including through analytics and business intelligence)	Legitimate interest - to understand how our products and services are used and improve them
To aggregate or deidentify data for analysis and produce insights about the use of our services and websites	Legitimate interest - to develop and enhance our offerings
To research, monitor, and evaluate our products and services in order to improve quality and develop new offerings	Legitimate interest - to innovate and enhance our service delivery

To monitor or audit your use of our products, services, and equipment for compliance with contractual terms or applicable law	Legitimate interest - to ensure compliance and protect our rights
To minimise the risk of or prevent fraud, crime, or misconduct	Legitimate interest - to protect our business, users, and partners
To enhance or ensure the safety and security of our and others' employees, customers, suppliers, and systems	Legitimate interest - to maintain a safe and secure environment
To help our partners (or other customers to whom we provide services on their behalf), such as antiabuse partners, to improve their services or online offerings	Legitimate interest - to support our partners' improvement and innovation activities
To send you educational information (e.g. scam education) related to the email service we provide to you	Legitimate interest - to help our customers learn how to protect their email accounts from bad actors
To develop, train, test, and improve artificial intelligence (AI) systems and features used in the delivery, operation, security, and improvement of our products and services (including customer support tools, user experience enhancements, and internal operational capabilities).	Legitimate interest - to enhance and improve our services, customer experience, and operational efficiency
As part of AI-driven processing, to analyse, summarise, categorise, and process communications, usage data, and interactions (including customer service enquiries, emails, and service usage patterns) to improve efficiency, personalise and enhance user experiences, support internal reporting and analytics, and maintain service quality and security.	Legitimate interest - to operate, improve, and secure our services and business

AI-driven processing safeguards

We may use artificial intelligence (AI) and automated processing tools to support and enhance our services, operations, security, and customer experience. All AI-driven processing is designed and implemented in accordance with applicable data protection laws and the principles of data minimisation and purpose limitation.

Personal data (including user prompts or communications) will not be used to train publicly available or third-party AI models. The use of personal data to train AI models is permitted only where the model is owned and operated by The Messaging Company or its related entities and is not exposed to unrelated third parties.

Where third-party AI tools or service providers are used, we require them to comply with appropriate contractual, security, and data protection obligations consistent with this Privacy Notice.

5. Sharing and disclosure of personal data

We may share your personal data with third parties, including to:

- a) our business partners and customers (e.g. partners or customers who we supply our goods and services to and who ask us on their behalf to supply them, as they may be providing their goods and services to you);
- b) members of our corporate group, which means our subsidiaries, our ultimate holding company and its subsidiaries;
- c) our suppliers, service providers, agents, contractors, and partners who assist us with our business processes and to provide our products and services, including in relation to:
 - i. helpdesk or chat services;
 - ii. information technology services;
 - iii. data processing, transfer, or hosting services;
 - iv. third-party products and service providers whose products and services you purchase from us or our customers;
 - v. providing, managing, supporting, and improving our websites, products, services and organisation;
 - vi. identity and fraud, or other crime protection services, credit reporting, or management services;
 - vii. business analysis and business intelligence services;
 - viii. customer relationship management system services;
 - ix. payment processing services; and
 - x. antiabuse services (e.g. antispam, antivirus, antimalware, and image classifiers, etc.);
- d) other persons authorised by you or who are responsible for or to you (such as guardians, persons holding power of attorney, lawyers, marketing partners, or executors);
- e) regulators, law enforcement, national security agencies, or courts;
- f) credit and debt collection services;
- g) our professional advisers, including consultants, lawyers, bankers, auditors, audit assessors, insurers, risk assessors, or accountants who provide consultancy, legal, banking, auditing, insurance, risk management, or accounting services;
- h) financiers, investors or third parties to whom we may choose to sell, transfer, or merge parts of our business or our assets or that we acquire businesses or merge with (if a change happens to our business, then the new owners may use your personal data in the same way as set out in this Privacy Notice and also to evaluate our business and whether to proceed with a transaction with us); and

- i) to third parties as required to protect the security or integrity of our services or to exercise or protect the rights, property, or personal safety of our company, our users, you, or others.

Any personal data you make publicly available on our websites or our service, such as posting comments on our blog page, in our forums, or on our websites, may be available to others to view. If you remove personal data that you have made public on our websites or on our service, copies may remain viewable in cached and archived pages of our websites or our service, or by other users who may have copied or saved that personal data.

6. International personal data transfers

Your personal data may be transferred to, stored in, or processed in, countries outside Australia, where we, our related entities, or our service providers operate. These locations may include:

- European Economic Area (EEA)
- United States of America
- Singapore
- Canada

Some of these locations may not have data protection laws equivalent to those in Australia or your country of residence. Where such transfers occur, we take reasonable steps to ensure they are carried out in compliance with applicable data protection laws and that appropriate safeguards are implemented to protect your personal data, unless an exception applies under applicable law.

Depending on the circumstances and the laws that apply, these safeguards may include contractual protections, reliance on adequacy or equivalency determinations, or other legally recognised transfer mechanisms.

We may transfer personal data to our affiliates, subsidiaries, and trusted service providers to support the operation and delivery of our services. Regardless of where your personal data is processed, we will take reasonable steps to ensure that it is handled in a manner consistent with this Privacy Notice and applicable privacy and data protection laws.

7. Personal data retention

We will retain your personal data while it is required for our business functions, or as is necessary to comply with our legal obligations, or to resolve disputes and/or enforce our agreements or rights under applicable laws. When we no longer need to retain your personal data for the purposes outlined above or as required by applicable law, our process is to destroy or deidentify the information.

8. Your rights

Accuracy. It is important that the personal data you have provided to us is up-to-date, accurate and complete. Please keep us informed if your personal data changes during your relationship with us. If your details change you can update your account by logging into your account to update your password, billing information, and other personal data.

Anonymous interaction. You have the option to engage with us anonymously. However, if you choose to interact with us anonymously, we may not be able to provide our products or services to you or make some offers available to you without your personal data.

Exercising your rights. Depending on your location and the applicable data protection or privacy laws, you may have certain rights in relation to the personal data we hold about you. These rights may include:

- **Access** - to request access to personal data we hold about you.
- **Rectification** - to request correction of any inaccurate or incomplete personal data.
- **Erasure** - to request deletion of your personal data in certain circumstances.
- **Restriction** - to request restriction of, or object to, certain processing activities in certain circumstances.
- **Portability** - to request a copy of your personal data in a portable format, where applicable.
- **Withdraw consent** - where processing is based on your consent, and where permitted by law, you may withdraw that consent at any time.

The availability and scope of these rights may vary depending on the law that applies to you, and we will assess and respond to each request in accordance with applicable legal requirements. We are not required to comply with a request where an exemption or limitation applies under applicable law.

To exercise any rights that may be available to you, please contact us using the details set out in this Privacy Notice.

Verification of identity and response times. We may need to request specific information from you to confirm your identity and to ensure your right to access your personal data (or exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to anyone who has no right to receive it. We aim to respond to all legitimate requests within one month. If your request is particularly complex or you have made multiple requests, we may take longer. In such cases, we will notify you and keep you informed of progress. We do not charge a fee for responding to your request unless we believe it is clearly unfounded, repetitive, or excessive, in which case we may charge a reasonable fee or refuse to act on the request. Where permitted by applicable law, we may refuse or charge a reasonable fee for requests that are manifestly unfounded, excessive, or repetitive.

Right to complain. If you believe we have not handled your personal data in accordance with applicable privacy or data protection laws, you may have the right to lodge a complaint with the relevant privacy, data protection, or consumer protection authority in your jurisdiction. The availability of this right, and the authority to which a complaint may be made, will depend on the laws that apply to you. If you are located in Australia and you are not satisfied with our response, you may also lodge a complaint with the Office of the Australian Information Commissioner (OAIC).

9. Security of your personal data

We implement appropriate technical and organisational measures, including industry-standard security controls, designed to protect personal data from loss, theft, misuse, and unauthorised access, disclosure, alteration, and destruction, taking into account the nature of the personal data processed, and associated risks. Examples include:

- **Encryption:** All data in transit is protected using TLS 1.2+ protocols, and data at rest is encrypted using AES-256 standards.
- **Access control:** System access is restricted by role-based permissions and enforced through multifactor authentication (MFA). Access is granted on the principle of least privilege.
- **Network security:** Firewalls, intrusion detection/prevention systems, and antimalware solutions are deployed to safeguard our infrastructure.
- **Physical security:** Access to data centres and corporate offices is controlled through secure entry systems, surveillance, and visitor management protocols.
- **Monitoring and logging:** Continuous monitoring of systems and logging of user activities, exceptions, and security events to detect and respond to anomalies promptly.
- **Incident response:** A formal incident response plan ensures rapid containment, investigation, and remediation of security incidents.
- **Vendor management:** Third-party providers undergo security assessments and must comply with contractual obligations, including encryption and data protection standards.
- **Regular audits and risk assessments:** Internal audits and vulnerability assessments are conducted to identify and mitigate risks proactively.

These measures are supported by ongoing staff training, documented policies (e.g. Data Classification, Acceptable Use, and Password Management), and independent audits, and are designed to align with recognised information security standards, including ISO/IEC 27001, and applicable data protection laws.

10. Children's privacy

We do not knowingly collect or solicit personal data from children or anyone under the age of eighteen (18) without the lawful authority to do so (such as consent of the parent or guardian). Please contact us if you believe we might have any personal data from or about a child or person under the age of eighteen (18) without lawful authority.

11. Direct marketing

While you are our customer, we may use your personal data from time to time to send you promotional material and direct marketing communications and information in relation to our products and services which we consider may be of interest to you. We do this by email, SMS, or other electronic messages or written notices, or through posting of such material on our services or our websites.

Opt-out options: You can opt out of receiving direct or electronic marketing communications from us at any time by using the opt-out facilities provided in the marketing communications or by contacting us at privacy@themessaging.co

Please note that opting out of marketing from us does not mean you will not be served advertisements online from third-party websites, or messages that may appear in your mailbox. You

may still see advertisements based on your browsing history, or untargeted advertisements, but you will not be served advertising nor be marketed to by us and we will not provide your details to any third party for marketing purposes.

12. Cookies

Our Cookie Policy at <https://themessaging.co/cookie-policy> provides you with information about how we collect, use, and disclose personal data through cookies.

13. Third-party links

Our websites may include links to other websites or applications provided by others, including those acting on our behalf. We are not responsible for the practices employed by websites or services linked to or from our services or websites, including the information or content contained therein. Clicking on those links or enabling those connections may allow third parties to collect or share data about you in accordance with their own privacy policies.

Your browsing and interaction on any third-party website or service, including those with a link or advertisement on our websites, are subject to that third party's privacy policies. You acknowledge that we do not control third-party websites, and we are not responsible for their privacy practices or policies. You should review the privacy policy of any third party and any applicable terms of use when you use their websites and applications.

14. Social media widgets

Our websites may include social media features (such as a Facebook Like button and/or other widgets) that run on our websites. These features may collect your IP address and which page(s) you visit on our websites and may set a cookie to enable the feature to function properly. Social media features and widgets are either hosted by a third party or hosted directly on our websites. Your interactions with these features are governed by the privacy policy of the organisation providing it.

15. Contact us

If you have any questions or concerns about your privacy, you may contact us via:

Privacy Officer
The Messaging Company Pty Ltd
Suite 251, Level 18, 324 Queen Street
Brisbane QLD 4000
Australia
privacy@themessaging.co

16. Changes to our Privacy Notice

We may update this Privacy Notice from time to time to reflect changes in our practices, legal requirements, or for other operational reasons. The date of the most recent update will always be shown at the top of this Notice.

Where changes are material, we will notify you in advance (e.g. by email or by posting a clear notice on our website) before the changes take effect.

Our Privacy Notice can be viewed online at <https://themessaging.co/privacy>