Privacy Policy

Logical Solutions Limited

Version 1.0 — Draft for legal review
Effective date: [DD Month 2026]
Last updated: 10 September 2026

1. About this policy

Logical Solutions Limited ("Logical Solutions", "we", "us", "our") is a managed IT services provider based in Hamilton, New Zealand.

This policy explains how we collect, use, store, disclose, retain and delete personal information in connection with:

- our website, sales and marketing activities;
- our managed IT services, helpdesk and support operations;
- our Data Warehouse service, which ingests and consolidates data from a customer's business systems ("data silos") into a hosted repository; and
- our Private AI / Business Intelligence Platform, which allows a customer's authorised users to query that consolidated data using artificial intelligence models operated by Logical Solutions.

It also explains how we handle data obtained from Meta Platforms, Inc. and its affiliates ("Meta") where our platform integrates with the WhatsApp Business Platform and other Meta products and APIs. **Section 8 applies specifically to Meta Platform Data** and, in the event of any inconsistency, Section 8 prevails in respect of that data.

This policy is published at a publicly accessible HTTPS address and does not require a login to view.

2. Key terms

Term	Meaning
Personal information	Information about an identifiable individual, as defined in the Privacy Act 2020 (NZ). Where other laws apply, it also carries the meaning of "personal data" under the UK/EU GDPR and "personal information" under applicable US state privacy laws.
Customer	A business that engages Logical Solutions to provide managed IT, Data Warehouse or Private AI Platform services.
Customer Data	Data belonging to or controlled by a Customer that is ingested into, stored in or processed by our Data Warehouse or Private AI Platform. This may include personal information about the Customer's own staff, clients, suppliers and contacts.
End User	An individual who interacts with a Customer through a channel we operate on the Customer's behalf, including an individual who messages the Customer via WhatsApp.
Meta Platform Data	Any data we obtain from Meta, or through a Meta API, product, SDK or business tool, including data about a Customer's Meta or WhatsApp Business Account and data about End Users.

3. Our role: controller and processor

Our role depends on the data:

- Where we act as the controller (a “collecting agency”): information we collect for our own purposes, including website enquiries, sales and account contacts, billing records, service tickets raised with us, and our own staff records. We decide how this information is used and we are directly accountable for it under this policy.
- Where we act as a processor (an “agent” of the Customer): Customer Data held in the Data Warehouse or processed by the Private AI Platform, and Meta Platform Data relating to a Customer’s End Users. Here the Customer is the controller. We process that data only on the Customer’s documented instructions, under a written services agreement and data processing addendum, and we do not use it for our own purposes.

Where we act as a processor, End Users should direct requests about their information to the relevant Customer in the first instance. We will assist the Customer in responding, and we will not respond to an End User’s request in a way that overrides the Customer’s instructions unless we are legally required to.

4. Information we collect

4.1 Information you give us directly

Name, business name, job title, email address, phone number, the content of your enquiry, and any information you include in correspondence with our sales or support teams.

4.2 Information collected through our website

IP address, browser and device type, pages visited, referring URL, and approximate location derived from IP address. See Section 14 (Cookies).

4.3 Information collected in the course of providing managed IT services

Support tickets, device and asset inventories, system and security logs, configuration data, and diagnostic information from Customer environments.

4.4 Customer Data ingested into the Data Warehouse

We ingest only the data sources a Customer instructs us to connect. Typical sources include:

- helpdesk and ticketing systems;
- document management and file repositories;
- accounting and finance systems (for example Xero);
- telephony platforms, including call detail records and, where enabled, call recordings and transcripts;
- email and calendar systems;
- CRM and quoting systems; and
- line-of-business applications specified during discovery.

The specific sources, fields and date ranges connected for each Customer are documented in that Customer’s discovery documentation and services agreement. Customers are responsible for ensuring they have a lawful basis for providing this data to us and for notifying the individuals concerned.

4.5 Information generated by the Private AI Platform

User account and authentication records, prompts submitted by authorised users, AI-generated responses, references to the source records retrieved to answer a query, timestamps, and audit logs of access and activity.

4.6 Meta Platform Data

See Section 8.

5. Sensitive information

We do not seek sensitive personal information — including health information, biometric or genetic data, government identifiers, financial account numbers, precise geolocation, racial or ethnic origin, religious or political beliefs, trade union membership, sexual orientation or sex life, or information about criminal convictions — for use in the Data Warehouse or Private AI Platform, and we instruct Customers not to send it to us unless it has been expressly scoped, documented and approved in writing as part of the service.

We never transmit sensitive information to Meta, and we do not include it in any data sent to Meta business tools.

6. How we use information

We use personal information only for the following purposes:

1. to respond to enquiries and provide quotes, proposals and letters of intent;
2. to deliver, configure, monitor, support and maintain the services a Customer has engaged us to provide;
3. to ingest, transform, index and store Customer Data in the Data Warehouse so that it can be queried;
4. to answer authorised users' queries through the Private AI Platform, including by retrieving relevant Customer records at the time a query is made;
5. to send and receive messages on a Customer's behalf through channels the Customer has authorised, including WhatsApp;
6. to secure our systems, investigate incidents, prevent fraud and abuse, and maintain audit trails;
7. to invoice and collect payment, and to maintain financial and tax records; and
8. to meet our legal, regulatory and contractual obligations.

Where the GDPR applies, our lawful bases are: performance of a contract (purposes 1–5, 7), legitimate interests (purposes 1, 6), legal obligation (purposes 7, 8) and, where required, consent. Where consent is the basis, it may be withdrawn at any time.

We do not sell personal information, and we do not share personal information for cross-context behavioural advertising.

7. Artificial intelligence: how our AI processing works

This section describes our AI processing because it is central to our services and because we want Customers and End Users to understand it.

Where the models run. The AI models used by the Private AI Platform run on infrastructure owned and operated by Logical Solutions in New Zealand data centres. Prompts, retrieved Customer records and generated responses are processed on that infrastructure. [If any third-party or hosted model is used for

any function, name the provider, the function, and the data sent to it here — otherwise delete this sentence.]

No training on your data. We do not use Customer Data, prompts, AI outputs, or Meta Platform Data (including WhatsApp message content) to train, fine-tune, develop, improve, evaluate or benchmark any artificial intelligence or machine-learning model, whether our own or a third party's. Data is used at inference time only — that is, to answer the query in front of it — and is not incorporated into model weights.

Separation between Customers. Each Customer's application instance and data stores are logically separated and run on dedicated virtual machines. Underlying compute resources, including GPU capacity, may be shared across instances; that sharing is at the compute layer only and does not give one Customer's instance access to another Customer's data or indexes.

Human access. Our engineers may access Customer Data, prompts and logs where necessary to configure, troubleshoot, secure or support the service. Access is role-based, individually authenticated, logged, and limited to what is required for the task.

Accuracy and human oversight. AI-generated output can be incomplete or incorrect. Output is presented to authorised users as decision support, not as a decision. We do not use the Private AI Platform to make automated decisions that produce legal effects for an individual or otherwise significantly affect an individual, and we do not permit Customers to configure it to do so.

Restricted purposes. We do not use the Data Warehouse or the Private AI Platform, and we do not permit them to be used, to make or inform eligibility decisions about individuals — including decisions about credit, insurance, employment, housing, tenancy, education, scholarships, immigration status or government benefits — or for surveillance, profiling of individuals for advertising purposes, or facial recognition.

8. Meta Platform Data (WhatsApp Business Platform and Meta APIs)

Logical Solutions is registered with Meta as a Tech Provider and operates a Meta application ("our App") that enables Customers to connect a WhatsApp Business Account and to send and receive WhatsApp messages through our platform. Our use of Meta Platform Data is governed by the Meta Platform Terms, the WhatsApp Business Solution Terms, the Meta Developer Policies and, where applicable, the Meta Business Tools Terms, in addition to this policy.

8.1 What we receive from Meta, and why

Data	Meta permission / product	Purpose
Business portfolio ID, WhatsApp Business Account (WABA) ID, phone number ID, display name and verification status	business_management, Embedded Signup	To onboard a Customer, link their WABA to our platform and configure their sender
System user access tokens and credentials	Embedded Signup	To authenticate API calls made on the Customer's behalf
Message templates, template status, category and quality ratings	whatsapp_business_management	To create, submit and monitor templates for the Customer
Phone number quality rating, messaging limits, account status	whatsapp_business_management	To monitor deliverability and warn the Customer of restrictions

Data	Meta permission / product	Purpose
End User phone number and WhatsApp profile name	whatsapp_business_messaging	To route inbound messages to the correct conversation and to send replies
Inbound and outbound message content, including text, media and attachments	whatsapp_business_messaging	To deliver the messaging service, maintain conversation history for the Customer, and — where the Customer has enabled it — to generate suggested or automated replies via the Private AI Platform
Message metadata: message IDs, conversation IDs, timestamps, delivery and read status, pricing category	whatsapp_business_messaging	Delivery confirmation, troubleshooting, audit trails and billing reconciliation

We request only the permissions listed above and we use each only for the purpose stated. We do not use Meta Platform Data for any purpose the End User or Customer would not reasonably expect from the description above.

8.2 What we will not do with Meta Platform Data

We will not:

- sell, licence, rent or otherwise transfer Meta Platform Data, or transfer it to any data broker, information broker or ad network;
- use it to create, augment or enrich a profile of an individual for advertising or targeting purposes, or transfer it to any advertising or monetisation platform;
- use it to make or inform eligibility decisions, including credit, insurance, employment, housing, education, immigration or government benefit decisions;
- use it for surveillance purposes, or provide it to law enforcement except where required by valid legal process;
- use it to train, fine-tune or improve any AI or machine-learning model (see Section 7);
- combine it with data from other sources except as necessary to provide the Customer with the service described in this policy and within that Customer's own tenant; or
- transfer it to any third party other than the sub-processors described in Section 9, each of which acts on our behalf under written contract.

8.3 Consent and opt-in for WhatsApp messaging

Customers must obtain each End User's opt-in before messaging them on WhatsApp, must make clear that the End User is opting in to receive messages from that Customer, and must keep records of that opt-in. Our platform records opt-in and opt-out events. End Users can opt out at any time by replying with a stop request to the conversation, by blocking the sender in WhatsApp, or by contacting the Customer directly.

8.4 Deletion of Meta Platform Data

We delete Meta Platform Data:

- when Meta or the Customer instructs us to;

- when a Customer disconnects their WhatsApp Business Account from our App, deletes their account, or terminates the service;
- when we receive a data deletion request through the data deletion callback we have registered with Meta, or through our published deletion instructions;
- when the data is no longer necessary for the purpose for which it was obtained; and
- where deletion is required by law.

Deletion instructions and our deletion request form are published at **https://logicalsolutions.co.nz/data-deletion**. We action verified requests within [30] days and confirm completion in writing. Where we act as a processor for a Customer, we will notify that Customer of the request and coordinate deletion with them.

9. Disclosure and sub-processors

We disclose personal information only:

- to the Customer whose data it is;
- to our sub-processors, listed below, each engaged under a written contract that limits them to processing on our instructions, prohibits use for their own purposes, requires equivalent security and confidentiality obligations, and requires deletion on our instruction;
- to Meta, where messages or configuration changes must be transmitted through Meta's APIs to deliver the service;
- where required or authorised by law, or in response to valid legal process; and
- to a purchaser in connection with a sale of our business, subject to the purchaser agreeing to comparable privacy obligations.

10. Where information is stored, and overseas disclosure

Customer Data, AI processing and the Private AI Platform are hosted in New Zealand. Some sub-processors listed in Section 9 are located outside New Zealand.

Before disclosing personal information outside New Zealand we take the steps required by information privacy principle 12 of the Privacy Act 2020 — that is, we satisfy ourselves that the recipient is subject to comparable privacy safeguards, or we bind the recipient by contract to comparable safeguards. Where the GDPR applies, transfers out of the EEA or UK rely on the European Commission's adequacy decision in respect of New Zealand, or on standard contractual clauses.

Messages sent through WhatsApp are transmitted through Meta's infrastructure and are handled outside New Zealand in accordance with Meta's own privacy policy and terms, which we do not control.

11. Retention

We keep personal information only for as long as we need it, and then delete or de-identify it.

Data	Retention
Website enquiries and sales contacts	[24] months from last contact, unless a contract results
Customer contract, billing and tax records	7 years, as required by NZ tax law
Support tickets and service records	Term of the agreement plus [12] months

Data	Retention
Customer Data in the Data Warehouse	As specified in the Customer's services agreement; deleted or returned within [30] days of termination
Prompts, AI outputs and query audit logs	[12] months, then deleted or de-identified
WhatsApp message content and metadata	[30] days in our operational store; longer only where the Customer has contracted for extended conversation history, and in no case beyond the term of the agreement plus [30] days
Meta access tokens and credentials	Until revoked, the account is disconnected, or the agreement ends
Security, access and system logs	[90] days, or longer where required for an active investigation
Backups	[35] days, after which deleted data is purged from backup media

Where we are required by law to retain information we would otherwise delete, we isolate it, stop actively processing it, and delete it once the obligation ends.

12. Security

We maintain administrative, physical and technical safeguards designed to meet or exceed industry standards for the sensitivity of the information we hold, to comply with applicable privacy and data security law, and to prevent unauthorised access, alteration, disclosure, loss or destruction. These include:

- encryption of data in transit (TLS 1.2 or higher) and at rest;
- role-based access control, unique named accounts and mandatory multi-factor authentication for all administrative access;
- logical separation of Customer environments, with per-Customer virtual machines and data stores;
- centralised logging, alerting and retention of audit trails;
- patch and vulnerability management, with periodic vulnerability assessment;
- documented change control, backup and disaster recovery procedures;
- background-checked personnel bound by confidentiality obligations, with privacy and security training; and
- an incident response plan that is tested periodically.

We complete Meta's Data Protection Assessment for our App where required, and we cooperate with Meta's audit and verification requirements under the Meta Platform Terms.

Breach notification. If a privacy breach occurs that is likely to cause serious harm, we will notify the Office of the Privacy Commissioner and affected individuals as required by the Privacy Act 2020. Where the breach affects Customer Data or Meta Platform Data, we will notify the affected Customer without undue delay, and we will notify Meta within the timeframe required by our agreement with Meta.

13. Your rights

Under the Privacy Act 2020 you may ask us to confirm whether we hold personal information about you, to give you access to it, and to correct it if it is wrong. Where the GDPR or a US state privacy law applies to our processing, you may also have rights to deletion, portability, restriction, objection, and to withdraw consent.

To make a request, contact our Privacy Officer using the details in Section 1, or use the form at https://logicalsolutions.co.nz/data-deletion for deletion requests. We will:

- acknowledge your request promptly and respond within 20 working days (Privacy Act) or one month (GDPR), and tell you if we need longer;
- verify your identity before acting, using the minimum information necessary; and
- tell you the reason if we decline any part of a request, and explain how to complain.

If your information is held by us on behalf of a Customer, we will tell you who that Customer is (where we are permitted to) and refer your request to them, or act on their instructions.

Making a request costs nothing in ordinary cases.

14. Cookies and website analytics

Our website uses cookies that are strictly necessary for it to function, and [analytics cookies / no analytics cookies]. Where consent is required in your jurisdiction, we ask for it before setting non-essential cookies, and non-essential cookies are off by default. You can control cookies through your browser settings.

[If Meta Pixel, Conversions API or offline conversions are used on our website, state that here, describe what is sent to Meta, and confirm that consent is obtained where required and that no sensitive information is transmitted. If they are not used, state that we do not use Meta business tools on our website.]

15. Children

Our services are provided to businesses and are not directed to children. We do not knowingly collect personal information from anyone under 16, and WhatsApp messaging through our platform is intended only for individuals who meet WhatsApp's minimum age requirement in their country. If we learn we have collected such information, we will delete it.

16. Changes to this policy

We will update this policy when our practices change. The version number and last-updated date at the top will change, and we will keep prior versions available on request. Where a change materially affects how we handle personal information, we will notify affected Customers in advance, and — where required — seek fresh consent before applying the change to information already collected.

17. Complaints

If you are not satisfied with our response, you may complain to:

Office of the Privacy Commissioner (New Zealand)

Freephone 0800 803 909 — enquiries@privacy.org.nz — www.privacy.org.nz

If the GDPR applies to you, you may also complain to your local supervisory authority.