Privacy Policy

Effective Date: 18 December 2025
Version: 1.1

1. Acronyms and definitions

In this Privacy Policy:

- **“JillAI”, “we”, “us”, “our”** means **JillAI (Pty) Ltd**, trading as **Jill.AI**
- **“IO”** means the **Information Officer**.
- **“PAIA”** means the Promotion of Access to Information Act 2 of 2000 (as amended).
- **“POPIA”** means the Protection of Personal Information Act 4 of 2013.
- **“Regulator”** means the Information Regulator (South Africa).
- **“Services”** means any website, application, product, platform, dashboard, or service that JillAI develops or operates and that displays or links to this Privacy Policy.
- **“IOkT”** means **Internet Of Kids Things**.
- **“IOkT Suite”** means the IOkT-related products and applications that JillAI develops or operates.
- **“Children”** means minors under 18 years old who use the Services.
- **“Guardians”** means parents or legal guardians who authorise a Child’s use of the Services.

2. Purpose of this Privacy Policy

This Privacy Policy explains:

- what personal information we collect and process;
- why we process it;
- who we share it with;
- where it is processed (including any cross-border processing);
- how we secure it; and

- what rights you have and how to exercise them.

3. Scope: which products and projects this policy applies to

3.1 Services covered

This Privacy Policy applies to all **Services** that JillAI develops or operates and that link to or reference this policy, including the **IOkT Suite**.

3.2 IOkT Suite

JillAI develops and operates IOkT and the IOkT Suite. The IOkT Suite is a multi-layered set of safety and security applications intended to protect minors in digital environments.

The IOkT Suite may change over time as we improve protections and release products in phases. Current planned products include **IOkT ID Secure**, **IOkT Net**, **IOkT Key**, and **IOkT Tutor**, which may roll out during 2026.

IOkT Tutor (high level): a supportive learning agent intended to run **local-first** wherever feasible. By default, we aim not to store a child's tutoring chats or audio on our servers, and we do not use Tutor activity for advertising or behavioral profiling.

3.3 Separate notices

If a specific Service has a separate privacy notice, that notice will apply to that Service.

3.4 Our operating standard

Where JillAI develops or operates additional products in future, JillAI intends to apply the privacy principles and protections described in this policy. If our processing changes, we will update this policy.

4. Key contact details (Privacy / POPIA)

Information Officer: Estelle Coetzee
Email: estelle.coetzee@jilldotai.co.za
Website: jilldotai.co.za
Address: Sasolburg, Freestate, South Africa, 1947

If you have an Information Regulator reference/registration number for the Information Officer process, add it here: `\[Insert reference number\]`.

5. Our “privacy-first” architecture (high level)

As a baseline principle:

> Before verification we process minimal security signals to protect the service. After verification (with guardian consent) we may process additional device signals to prevent fraud and keep children safe. We do not use these signals for advertising.

For example, we may process limited technical information (such as IP address and security logs) to prevent abuse and keep the Services secure. We aim to avoid collecting or retaining real-world identity information about Children unless a Guardian explicitly chooses a specific workflow that requires it, and we will limit any such processing to that purpose.

We build IOkT and our Services with a privacy-first, safety-by-design approach.

- **On-device processing where possible:** We aim to perform safety analysis locally on the device to minimise centralised collection.
- **Data minimisation:** We aim to collect only what we need to provide safety features, account security, and legal compliance.
- **Transparency:** We describe categories of processing in this policy and update it when processing changes.

6. Categories of personal information we process

6.0 Waitlist / sign-up information (Guardian-led)

If you sign up for early access, testing updates, or launch announcements, we may process the contact information you submit (for example, name and email). This information is typically captured into an internal spreadsheet or similar system used for communications and coordination.

We use this contact information to:

- send operational updates about testing phases, access, and product changes; and
- send launch announcements.

If you unsubscribe, we remove you from the relevant communications list so that we do not send further updates (subject to any limited records we may need to keep to respect your opt-out request).

6.0.1 Anonymous research survey responses

We may also run separate research surveys to understand what Guardians want and where pain points exist.

Where we describe survey responses as “anonymous,” we mean:

- the survey responses are collected separately from waitlist contact details; and
- we do not link survey responses back to identifiable individuals.

We use these anonymous survey responses for internal research and product improvement.

6.1 Information about Guardians (provided by you)

We may process:

- contact information (name, email, phone number);
- account identifiers and authentication data;
- verification signals used to confirm adult/Guardian status (which may include biometric liveness or other verification methods, depending on the provider and method chosen).

6.2 Information processed about Children (for safety)

Depending on the Service and settings, we may process:

- device and app information (device model, OS version, unique identifiers);
- app usage information needed to provide safety controls;
- safety-related signals and alerts generated by on-device analysis.

Important: We aim not to collect or store raw content such as keystrokes or full chat logs on our servers. Where a feature would require server-side processing, we will disclose it clearly in the relevant Service notice and/or update this policy.

6.3 Technical information

We may process:

- log data (e.g., IP address, timestamps, security events);
- diagnostic information (crash logs, performance data);
- anti-fraud and abuse-prevention signals.

7. Purpose of processing (why we use the information)

We process personal information to:

- create and manage Guardian and Child accounts;
- provide safety features (including detection of harmful content and threats);
- prevent abuse, fraud, and ban evasion;
- deliver alerts and reporting to Guardians where appropriate;
- maintain, secure, and improve the Services; and
- comply with legal obligations.

8. Consent and children’s information

8.1 Verification methods (how we verify Guardians and issue age-band credentials)

To protect Children and keep adults out of child-directed areas, JillAI may offer one or more verification methods for Guardians.

Default approach (document + selfie / liveness): A Guardian may be asked to submit an identity document (such as an ID document, driver’s licence, or passport) and complete a selfie / liveness check. We use automated checks to detect tampering or forged documents and to confirm consistency between submitted information and the document.

Security and fraud checks (risk scoring): During verification, we may run security and fraud-prevention checks (for example, IP and device risk signals) to detect abuse (such as automated sign-ups, VPN/proxy abuse, or other suspicious patterns). These checks are used to protect the Service and may increase friction (for example, requiring additional confirmation). They are not used for advertising.

Authoritative database checks (where available): In some cases (for example, in higher-assurance workflows, or where a Guardian explicitly selects a method that requires it), we may use regulated third-party services or authoritative sources to confirm submitted details. Where used, we aim to process the minimum information required to obtain a confirmation result (e.g., match/no-match).

Outcome: Where a Guardian successfully completes verification, JillAI issues an age-band credential for the Child (for example, 9–12) and applies safety controls accordingly. We aim to avoid collecting or retaining real-world identity information about Children beyond what is needed for the verification outcome, security/audit purposes, and legal compliance.

Where required by POPIA (including section 35) and other applicable laws, we require verified Guardian authorisation/consent before processing a Child's personal information.

9. Sharing: recipients or categories of recipients

We may share limited personal information with trusted operators and service providers to operate the Services, including:

- identity / age / adult verification providers (as applicable);
- fraud and risk providers (e.g., MaxMind / LexisNexis, if used);
- cloud infrastructure and hosting providers (e.g., Huawei Cloud and/or Google Cloud, if used);
- blockchain/credential infrastructure providers (e.g., Polygon-based identity infrastructure), where applicable.

We do not sell, rent, or trade personal information to advertisers.

10. Cross-border processing (planned transborder flows)

We operate primarily from **South Africa**. Depending on the providers we use, personal information may be processed or stored in South Africa and/or other countries where our service providers operate.

Where cross-border processing is required, we will implement appropriate safeguards and contractual protections consistent with applicable law.

11. Storage, retention, and deletion

We keep personal information only for as long as necessary for the purposes described in this policy, unless a longer period is required or permitted by law.

Guardians may request deletion of account data, subject to security and legal retention requirements.

12. Information security measures

We implement security safeguards appropriate to the sensitivity of the information, which may include:

- encryption in transit and at rest (where data is stored);
- access controls and least-privilege permissions;
- audit logging and monitoring;
- secure key management where applicable; and
- incident response procedures.

13. Your rights

Subject to applicable law, you may request:

- access to personal information we hold;
- correction/rectification;
- deletion/erasure (where applicable);
- objection to certain processing; and
- a copy of your information in a usable format where applicable.

To exercise these rights, contact the Information Officer using the details above.

14. Updates to this policy

We may update this Privacy Policy from time to time. We will revise the effective date and version number when we publish changes.

15. PAIA access to records (separate document)

Requests for access to records under **PAIA** are handled via our PAIA Manual. This Privacy Policy is not a PAIA Manual.