



PRIVACY POLICY

Casia Africa (Pty) Ltd — casia.africa, its subdomains and the Casia applications

Legal Document – CASIA

Document Field	Detail
Document	Privacy Policy
Issued by	Casia Africa (Pty) Ltd
Registration number	2025/009960/07
Version	1.0
Effective date	23 April 2026
Last reviewed	10 September 2026
Physical address	First Floor, 353 Festival Street, Hatfield, Pretoria
Website	www.casia.africa
General enquiries	hello@casia.africa
Information Officer	privacy@casia.africa
Next review	Twelve months from last review, or earlier if the law or our practices change

Plain-language summary: We collect only the personal information we need to run the Casia Platform and products. We never sell your personal information. Health, children's and financial information receives heightened protection. You have the right to see, correct, delete and object to our use of your information, and to complain to the Information Regulator. Details below.

This Privacy Policy is issued in terms of section 18 of the **Protection of Personal Information Act 4 of 2013 ("POPIA")** and, where applicable to users outside South Africa, Articles 13 and 14 of the EU/UK General Data Protection Regulation ("**GDPR**") and other applicable data-protection laws.



1. Who is responsible for your information

1.1 Responsible party: Casia Africa (Pty) Ltd , Tshwane, Gauteng, South Africa ("**Casia**", "**we**", "**us**").

1.2 Information Officer (registered with the Information Regulator in terms of section 55 of POPIA):

Email	privacy@casia.africa
-------	----------------------

1.3 EU/UK representative (only if we offer services to, or monitor, persons in the EU/UK and have no establishment there — Article 27 GDPR): [Name and address, or "Not currently appointed"].

1.4 When Casia is an operator, not the responsible party. When a healthcare practice, school, business, NGO or public body ("**Organisation**") uses a Casia product to manage its own patients, learners, customers, staff or community members, that Organisation is the responsible party and Casia processes that information only on its documented instructions as an **operator** (section 21 of POPIA / "processor" under GDPR). In that case the Organisation's privacy notice governs, and you should direct rights requests to the Organisation. Casia will assist the Organisation in responding. Sections 3–6 of this Policy describe our own processing as responsible party; section 12 describes our operator commitments.

2. Scope

This Policy applies to personal information processed through casia.africa and all subdomains, the Casia mobile and web applications, APIs, and all Casia products (Casia Care, Casia Spark, Casia Peyton, Casia Madibaz, Casia Safe, Casia Voice, Casia Horizon, Casia Roots, Casia Hearth, Casia Bonds and any future products), and to our dealings with website visitors, account holders, professionals, partners, suppliers, job applicants and other contacts.

3. What personal information we collect

We collect personal information in the following categories. "Personal information" has the meaning in section 1 of POPIA and includes information about identifiable natural persons and, where applicable, juristic persons.

3.1 Information you give us

Category	Examples
Identity and contact	Name, surname, ID/passport number (where verification is required), date of birth, email, phone number, physical address, profile photograph
Account and credentials	Username, hashed password, MFA settings, security questions, role and permissions
Professional and Organisation details	Practice/school/company name, registration numbers (CIPC, HPCSA, SACE, SARS), position, professional qualifications, B-BBEE and compliance documents (Casia Madibaz)
Financial and billing	Bank account details for debit orders, DebiCheck mandates, card token (not full card number), billing address, VAT number, transaction history, tax and financial statements uploaded for capital-readiness assessment
Communications	Emails, support tickets, chat messages, survey responses, partnership and press enquiries, call recordings (with notice)
Content you upload	Documents, images, notes, reports and other data submitted to the Platform
Recruitment	CV, references, qualifications, criminal-record and credit checks (with consent, where lawful)



3.2 Special personal information (section 26 of POPIA)

Depending on the product, we may process the following **special personal information**, only where a lawful ground in section 27 exists (usually your explicit consent, or where processing is necessary for the establishment of a right or obligation in law, or is carried out by/under the responsibility of a health professional bound by confidentiality):

- **Health information** (Casia Care): medical history, conditions, medication, clinical notes, referrals, community health-worker visit records, screening results, disability status. Health information is also protected by sections 14–17 of the National Health Act 61 of 2003 and, where relevant, the Mental Health Care Act and the Children's Act.
- **Biometric information**: only if you enable biometric login on your own device (processed on-device by your device's operating system) or where an Organisation configures biometric verification.
- **Race or ethnic origin**: only where required for B-BBEE reporting, statutory reporting, or where you voluntarily provide it for impact measurement.
- **Criminal behaviour**: only in Casia Safe incident reporting or vetting of certain roles, where lawful.
- **Religious or philosophical beliefs, political persuasion, trade union membership, sex life**: we do not deliberately collect these. Do not submit them unless a product specifically and lawfully requests them.

3.3 Children's personal information (sections 34–35 of POPIA)

Casia Spark, Casia Peyton and certain healthcare and community products may involve the personal information of children (persons under 18). We process children's information **only** with the consent of a competent person (parent or legal guardian), or where an Organisation (such as a school or clinic) has lawfully obtained such consent, or where another exception in section 35 applies (e.g. necessary for the establishment, exercise or defence of a right or obligation in law, or with authorisation of the Information Regulator). We apply data minimisation, restricted access, no behavioural advertising, and no profiling of children for marketing purposes.

3.4 Information collected automatically

Category	Examples
Device and technical	IP address, device type and identifiers, operating system, browser type and version, language, screen size, mobile network
Usage	Pages viewed, features used, clicks, time on page, referring URLs, crash reports, API call logs
Location	Approximate location from IP address; precise GPS location only with your device-level permission and only for features that need it (e.g. Casia Safe incident location, Casia Care community visits)
Cookies and similar technologies	See our Cookie Policy

3.5 Information from third parties

- Organisations that register you as a user (e.g. your employer, school, practice);
- Identity, professional-registration and business verification services (e.g. Home Affairs verification providers, CIPC, HPCSA, SACE, SARS eFiling where you link it);
- Payment service providers, banks and account-verification services (AVS);
- Credit bureaux (Casia Madibaz capital-readiness, only with your consent and in compliance with the National Credit Act);
- Public sources and partners (e.g. Department of Health, Department of Basic Education, municipalities, NGOs) under written data-sharing agreements;
- Social media platforms, where you interact with our pages or log in via a social account.



4. Why we process personal information and the lawful basis

Purpose	Lawful basis (POPIA s 11 / GDPR Art 6)
Creating and managing your account; providing the product you requested	Performance of a contract
Routing information between appropriate participants through the Casia data fabric (e.g. connecting a patient to a professional, a learner to an educator)	Contract; legitimate interests; consent for special/children's information
Identity, professional and business verification; fraud prevention	Legal obligation (FICA, NHA, HPA); legitimate interests
Billing, debit-order collection, payments and accounting	Contract; legal obligation (Companies Act, Tax Administration Act)
Customer support and communications about the service	Contract; legitimate interests
Security, monitoring, logging, incident response	Legal obligation (POPIA s 19); legitimate interests
Product improvement, analytics and research (de-identified where possible)	Legitimate interests; consent (analytics cookies)
Impact measurement and public reporting (aggregated/de-identified only)	Legitimate interests
Direct marketing to existing customers about similar products	Legitimate interests with opt-out (POPIA s 69(3)); otherwise consent
Direct marketing to non-customers / electronic marketing	Consent (POPIA s 69(2); ECTA s 45)
Compliance with law, court orders, regulators; establishing or defending legal claims	Legal obligation; legitimate interests
Recruitment	Pre-contractual steps; legitimate interests; consent for checks

Legitimate interests means processing necessary for our legitimate business interests where those interests are not overridden by your rights. You may object under section 11(3) of POPIA (see section 9).

5. Who we share personal information with

We do **not** sell personal information. We share it only as follows:

- 5.1 Operators (service providers)** who process information on our behalf under written operator agreements (section 21 of POPIA), including: cloud hosting and storage; email, SMS and WhatsApp messaging providers; payment processors, banks and debit-order system operators; identity-verification and AVS providers; analytics and error-monitoring providers; customer-support tooling; security and backup providers. A current list of sub-operators is available on request from the Information Officer.



- 5.2 Organisations and participants in the Casia ecosystem** — only the information needed for the specific purpose and only to participants authorised by the applicable access rules (for example, a referral is shared with the receiving healthcare professional; a learner's progress is shared with the school and consenting parent). The Casia data-routing fabric enforces purpose- and role-based access controls.
- 5.3 Partners** (private sector, public sector and NGO partners) under written data-sharing agreements, where you or your Organisation has agreed to participate in a partnered programme.
- 5.4 Regulators, law enforcement, courts and government bodies** where required by law (e.g. Information Regulator, SARS, FIC, SAPS under a lawful request, the Department of Health for notifiable conditions).
- 5.5 Professional advisers** (auditors, lawyers, insurers) under confidentiality obligations.
- 5.6 Corporate transactions** — a prospective purchaser or successor in a merger, acquisition or restructuring, under confidentiality, with notice to you where required.
- 5.7 With your consent** for any other purpose.

6. Cross-border transfers (section 72 of POPIA)

- 6.1** Casia's primary hosting is located in **South Africa**. Some service providers (e.g. email delivery, analytics, support tooling) may process information in other countries.
- 6.2** We transfer personal information outside South Africa only where: (a) the recipient is subject to a law, binding corporate rules or a binding agreement providing substantially similar protection to POPIA (we use contractual clauses aligned to POPIA Chapter 3 and, where relevant, EU Standard Contractual Clauses); (b) you consent; (c) it is necessary for the performance of a contract with you or in your interest; or (d) another ground in section 72(1) applies.
- 6.3** Health information of South African residents is stored in South Africa unless you or your Organisation expressly agrees otherwise.

7. How long we keep personal information (section 14 of POPIA)

We keep personal information only as long as necessary for the purposes collected, or as required by law, after which it is deleted or de-identified. Indicative periods:

Information	Retention
Account information	Duration of account + 5 years (limitation/prescription period)
Health records (Casia Care, where Casia is responsible party)	Minimum periods required by the HPCSA and National Health Act (generally not less than 6 years from date of last entry; longer for children and certain conditions)
Children's education records	Duration of enrolment + period required by the school/Department of Basic Education; then de-identified
Financial, tax and transaction records	5 years (Tax Administration Act; Companies Act; FICA)
Debit-order mandates	Duration of mandate + 5 years (PASA/PayInc rules)
Marketing consents and opt-outs	Until withdrawn; opt-out records kept indefinitely to honour them
Support communications	3 years
Security and access logs	12–24 months
Recruitment (unsuccessful applicants)	6 months unless consent to keep longer



Information	Retention
Backups	Rolled off within [90] days of deletion from live systems

Where Casia acts as operator, retention is determined by the Organisation.

8. How we protect personal information (section 19 of POPIA)

We maintain appropriate, reasonable technical and organisational measures, informed by ISO/IEC 27001 and the POPIA Regulations, including: TLS 1.2+ encryption in transit and AES-256 encryption at rest; role- and purpose-based access controls enforced by the Casia data-routing fabric; multi-factor authentication for staff and privileged users; network segmentation and firewalls; logging, monitoring and intrusion detection; regular vulnerability scanning and independent penetration testing; secure development lifecycle; staff confidentiality undertakings and training; business continuity and tested backups; operator due diligence and contractual security obligations. Payment-card data is handled by PCI DSS-compliant processors.

No system is perfectly secure. If we become aware of a security compromise affecting your personal information we will notify the Information Regulator and you as required by section 22 of POPIA, as soon as reasonably possible.

9. Your rights

Under POPIA (and, where applicable, GDPR) you have the right to:

- **Be notified** that your information is being collected or has been accessed by an unauthorised person;
- **Access** — request confirmation of whether we hold your personal information and a copy of it (section 23; PAIA Form 2 may be required — see our PAIA Manual);
- **Correction or deletion** — request that inaccurate, irrelevant, excessive, outdated, incomplete, misleading or unlawfully obtained information be corrected or deleted (section 24; Form 2 of the POPIA Regulations);
- **Object** — to processing based on legitimate interests, and to direct marketing at any time (section 11(3), 69; Form 1);
- **Withdraw consent** — where processing is based on consent, without affecting prior lawful processing;
- **Not be subject to solely automated decisions** with legal or similarly significant effect (section 71);
- **Data portability** (GDPR users) and **restriction of processing** (GDPR users);
- **Complain** to the Information Regulator (South Africa) or your local supervisory authority.

How to exercise your rights: email privacy@casia.africa, or use the in-app privacy settings. We may need to verify your identity. We respond within **30 days** (extendable once by 30 days where lawful). Access requests are free for confirmation of holdings; a prescribed fee may apply to copies. We will not discriminate against you for exercising your rights.

Information Regulator (South Africa): JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001 | complaints.IR@justice.gov.za | enquiries@infoeregulator.org.za | <https://infoeregulator.org.za>

10. Direct marketing

We send electronic marketing only (a) to existing customers about our own similar products, with an opt-out in every message, or (b) with your prior consent obtained in the form prescribed by the POPIA Regulations. You may opt out at any time via the unsubscribe link, in-app settings, or privacy@casia.africa. We do not send marketing to children and do not use children's information for marketing or profiling.

11. Cookies and tracking

See our Cookie Policy for details of the cookies we use and how to manage your preferences via the **Cookie Settings** link in the website footer. Non-essential cookies are not set until you consent.



12. Casia as operator — commitments to Organisations

Where Casia processes personal information on behalf of an Organisation, Casia: (a) processes only on documented instructions; (b) binds staff to confidentiality; (c) implements section 19 security measures; (d) engages sub-operators only under equivalent written terms and informs the Organisation of changes; (e) assists with data-subject requests and impact assessments; (f) notifies the Organisation without undue delay of any security compromise; (g) returns or deletes information at the end of the engagement unless retention is required by law; and (h) makes available information necessary to demonstrate compliance and permits audits on reasonable terms. These commitments are set out in full in Casia's Data Processing / Operator Agreement.

13. Users outside South Africa

If you are in the **EU/UK**, references to POPIA rights include your GDPR rights; the lawful bases in section 4 map to Article 6 and (for special categories) Article 9 GDPR; international transfers are made under Chapter V safeguards; and you may complain to your local supervisory authority. If you are in another African country (e.g. Nigeria, Kenya, Ghana, Botswana, Namibia, Zimbabwe, Mauritius), you may have additional rights under local data-protection law; contact the Information Officer to exercise them. If you are in **California**, we do not "sell" or "share" personal information as defined in the CCPA/CPRA, and we honour Global Privacy Control signals.

14. Third-party sites and services

Links to third-party websites, apps and services are provided for convenience; their privacy practices are governed by their own policies.

15. Changes to this Policy

We may update this Policy. Material changes will be notified by email or in-Platform notice at least 30 days before they take effect, except where a change is required by law sooner. Prior versions are available on request.

16. Contact and PAIA

Information Officer: privacy@casia.africa. Our **PAIA Manual** (Promotion of Access to Information Act 2 of 2000, section 51) is available at <https://casia.africa/legal/paia-manual> and at our offices.

Casia Africa (Pty) Ltd. , Tshwane, Gauteng, South Africa.