BEANTECH (PTY) LTD t/a OATHS.CO.ZA™

Parent / Legal Guardian Consent Notice

For users aged 16 and 17 – what you are consenting to, and how to withdraw it

Operator	Beantech (Pty) Ltd, registration number 2010/008997/07
Version	2.0 – 14 October 2026
Replaces	Version 1.0 (19 October 2025), which is withdrawn
Information Officer	Mr J.M. van der Westhuizen, compliance@oaths.co.za

1. Why this notice exists

A person under 18 is a child in law. Section 34 of the Protection of Personal Information Act 4 of 2013 ("POPIA") prohibits the processing of a child's personal information unless one of the grounds in section 35 applies. The ground Oaths.co.za™ relies on is **the prior consent of a competent person** – section 35(1)(a) – meaning you, as the parent or legal guardian.

This notice tells you what will happen to your child's information so that your consent is informed. POPIA requires consent to be voluntary, specific and informed. If any part of this notice is unclear, please ask before you consent.

It should be read with our **Privacy Policy**, **Terms and Conditions**, **Prohibited Use Policy** and **PAIA Manual**.

2. Who may use the platform

Oaths.co.za™ may be used by a person aged **16 or 17** who holds a valid South African Smart ID Card, and only where a parent or legal guardian has given verifiable consent **before** registration.

2.1 The recommended route – guardian first

We recommend that you register your own verified Oaths.co.za™ account first, and then invite your child to join through the secure onboarding flow. This gives you direct oversight of what is certified, makes consent easier to manage and withdraw, and simplifies verification.

2.2 Direct registration by the minor

A person aged 16 or 17 may also register directly, provided they hold a valid Smart ID Card and you provide verifiable digital consent through the secure consent process before the account becomes active.

3. What you are consenting to

By giving consent you confirm that you understand and agree to the following.

3.1 Purpose

- Your child's information will be processed for the certification of true copies of supported documents, and for the identity verification, record-keeping, payment, security and support functions that go with it. It will not be used for anything else, and it will not be sold or used for advertising.

3.2 Identity and biometric checks

Your child's face will be captured and checked, and you are consenting to that specifically. Before any document is certified we verify that the person is who they say they are. This involves checking the identity document against Department of Home Affairs records and performing a **biometric liveness check** on a facial image, to confirm a real, living person who matches the document. Biometric information is **special personal information** under section 26 of POPIA and may be processed only with **explicit consent under section 27(1)(a)**. Your consent to this is sought separately and expressly, and may be refused.

- The liveness check establishes only that the person is real and matches the identity document. It is used for nothing else.
- If you refuse, we cannot verify identity to the standard this service requires and we cannot certify documents for your child.

3.3 Where the checks happen – please read this

Part of this check takes place outside South Africa. The platform and your child's records are hosted on Microsoft Azure in the **South Africa North** region. However, identity verification and the biometric liveness check are performed by **Didit**, our verification partner, which processes in the **European Union** under the General Data Protection Regulation. What is sent to Didit is limited to the identity document details and the facial image captured for the check. Certified documents and certification records are **not** sent. Section 72 of POPIA permits this transfer with consent, and by consenting you also consent to it. You may refuse, in which case we cannot proceed.

Didit acts as our operator under a written data processing agreement, may process only on our instruction, and the verification session is deleted once the result has been received.

3.4 Security and separate handling

- Personal information is encrypted in transit and at rest, and access is controlled and logged.
- Certification records are written to a tamper-evident ledger and to write-once storage, so that they cannot be altered afterwards.
- **Additional safeguards apply to the information of users aged 16 and 17**, including restricted access and separate handling.

3.5 How long information is kept, and the limit on deletion

Please read this before consenting. Certification records are written to storage that cannot be altered or deleted until the retention period expires – **7 years**. This is deliberate: it is what makes a certified document trustworthy afterwards. It means that **if you withdraw consent, we will stop processing and close the account, but we cannot delete certification records already created** before that period ends. Section 14 of POPIA permits retention where it is required for a lawful purpose. We would rather tell you this now than promise a deletion we cannot perform.

4. Withdrawing your consent

You may withdraw your consent at any time, free of charge, by e-mailing **compliance@oaths.co.za** from the address on record, or by using the consent controls in your account.

- We will stop further processing of your child's personal information.
- We will restrict or close the minor's account.

- Withdrawal does not affect the lawfulness of anything done before it.
- Records we are required to keep are retained as described in section 3.5.

5. Your rights, and your child's

You may exercise the following on your child's behalf, and your child may exercise them too where able to do so:

- ask what personal information we hold, and ask for a copy;
- ask us to correct information that is inaccurate, incomplete or out of date;
- ask us to delete information, subject to section 3.5;
- object to processing we base on legitimate interests;
- withdraw consent; and
- complain to our Information Officer or to the Information Regulator.

Information Officer	Mr J.M. van der Westhuizen – compliance@oaths.co.za
Information Regulator (South Africa)	Woodmead North Office Park, 54 Maxwell Drive, Woodmead, Johannesburg, 2191
	Tel 010 023 5200 | Toll free 0800 017 160 | enquiries@inforegulator.org.za | inforegulator.org.za

6. Legal basis

Legislation	Relevance
Protection of Personal Information Act 4 of 2013	Section 11 – lawful grounds for processing. Section 18 – notification to data subjects. Section 19 – security safeguards. Sections 26 and 27(1)(a) – special personal information and explicit consent. Sections 34 and 35(1)(a) – the personal information of children and the consent of a competent person. Section 72 – transfer outside the Republic.
Children's Act 38 of 2005	Parental responsibilities and rights, and the authority of a guardian to assist and consent on a child's behalf.
Electronic Communications and Transactions Act 25 of 2002	Sections 13 and 15 – recognition of electronic signatures and the admissibility of data messages, so that consent given electronically is valid and can be evidenced.
Justices of the Peace and Commissioners of Oaths Act 16 of 1963	The authority under which the Commissioner of Oaths certifies a copy as a true copy of the original.

7. Guardian consent

I, the undersigned parent or legal guardian of the minor named below, give consent for that minor to register for and use Oaths.co.za™.

I confirm that:

(a) I am the parent or legal guardian of the minor and am authorised to give this consent;

(b) the minor is at least 16 and under 18 years of age and holds a valid South African Smart ID Card;

(c) I have read and understood this notice and the Privacy Policy, and I have had the opportunity to ask questions;

(d) I give my **explicit consent**, for the purposes of section 27(1)(a) of POPIA, to the biometric liveness check described in section 3.2;

(e) I give my consent, for the purposes of section 72 of POPIA, to the transfer described in section 3.3 of the identity document details and facial image to our verification partner in the European Union;

(f) I have read and accept the Minor Digital Pledge on the minor's behalf;

(g) I understand that certifications are recorded in a tamper-evident audit trail and that the records cannot be deleted before the retention period in section 3.5 expires; and

(h) I accept responsibility for supervising the minor's lawful use of the service.

Minor's details

Full name and surname	
Identity number	
Date of birth	

Guardian's details and signature

Full name and surname	
Identity number	
Relationship to the minor	
E-mail address	
Mobile number	
Signature	
Signed at	
Date	

Consent may also be given electronically, by checkbox or electronic signature, in accordance with sections 13 and 15 of the Electronic Communications and Transactions Act 25 of 2002. Where it is, the platform records the consent wording version accepted, the method of authentication, the date and time, and seals that record against alteration.

8. Revision history

Version	Date	Summary of change
1.0	19 October 2025	Initial publication. **Withdrawn.**
2.0	14 October 2026	Corrected and reissued. The statement that all data including biometric information is “ring-fenced within Microsoft Azure Confidential Ledger, hosted exclusively in South Africa” is removed: it was inaccurate. Processing of the facial image by the verification partner in the European Union is now disclosed, with consent sought under section 72. Biometric processing is identified as special personal information requiring explicit consent under section 27(1)(a). The ground for processing a child’s information is stated as section 35(1)(a). The limit on deletion imposed by the retention lock is disclosed. The registration number previously shown has been removed pending verification. References to the Financial Intelligence Centre Act removed.