Oaths.co.za – Prohibited Use Policy

Effective Date: 14 October 2026 | Version 2.1

1. Introduction and Legal Context

Oaths.co.za operates as a digital platform facilitating the digital certification of true copies by duly appointed Commissioners of Oaths in South Africa. Given the platform's role in legal documentation—a sector governed by strict statutory, ethical, and professional obligations—this Prohibited Use Policy establishes a rigorous compliance framework aligned with South African statutory law, including but not limited to:

- The *Justices of the Peace and Commissioners of Oaths Act 16 of 1963*
- The *Electronic Communications and Transactions Act 25 of 2002 (ECTA)*
- The *Protection of Personal Information Act 4 of 2013 (POPIA)*
- The *Prevention and Combating of Corrupt Activities Act 12 of 2004 (PRECCA)*
- The *Cybercrimes Act 19 of 2020*
- The *Consumer Protection Act 68 of 2008 (CPA)*
- The *Prevention of Organised Crime Act 121 of 1998 (POCA)*

This Policy outlines the strict boundaries governing user behavior, document submission, and interaction with the platform to prevent legal liability, protect system integrity, and ensure statutory compliance.

2. Core Prohibited Uses and Legal Frameworks

2.1 False or Misleading Document Certification

Users are strictly prohibited from submitting forged, altered, or fraudulent documents for certification, or presenting misleading information regarding the origin, authenticity, or content of a document.

- **Legal Basis:** Section 10 of Act 16 of 1963. Knowingly processing a false document or producing a fraudulent certification constitutes perjury and cyber forgery under Section 8 of the *Cybercrimes Act 19 of 2020*.
- **System Enforcement:** Automated document integrity checks, metadata analysis, and mandatory biometric matching.

2.2 Unauthorized Use of Commissioner Credentials

Users may not impersonate a Commissioner of Oaths, use stolen or misappropriated credentials, or attempt to access the platform's administrative or Commissioner-specific backend portals.

- **Legal Basis:** Section 86 of *ECTA* (unauthorized access to data systems) and identity theft provisions within common law.
- **System Enforcement:** Multi-Factor Authentication (MFA), strict IP tracking, and continuous session monitoring.

2.3 Exceeding Statutory Authority

The platform may **only** be used for the certification of true copies of acceptable source documents. Users are prohibited from utilizing the platform to process:

- Affidavits or sworn declarations requiring in-person commissioning (unless explicit live video-verification protocols are legislated and active).
- Documents requiring formal **Notarization** (which legally requires a Notary Public).
- Documents requiring **Apostille or Legalisation** for international use via DIRCO.
- **Legal Basis:** *Justices of the Peace and Commissioners of Oaths Act 16 of 1963* and the *Notaries Act 57 of 1997*.

2.4 Unauthorized Use by Minors

Users under the age of 18 are prohibited from utilizing the platform independently. Minors aged 16–17 may access services only via verified legal guardian interaction.

- **Legal Basis:** Section 18 of the *Children's Act 38 of 2005* (contractual capacity restrictions) and Section 35 of *POPIA* (processing of children's data).

2.5 Bulk Processing and Automated Misuse

The use of scrapers, bots, automated scripts, or batch-uploading tools to process documents without individualized manual review is strictly prohibited. Commercial resale of certifications issued via Oaths.co.za is forbidden.

- **Legal Basis:** Section 73 of *ECTA* and the *Copyright Act 98 of 1978* (protecting proprietary digital verification marks and security QR layouts).

2.6 Document Tampering and Verification Circumvention

Users are prohibited from modifying, flattening, obscuring, or separating the digital certification marks, cryptographic signatures, or tracking QR codes generated by the platform. Bypassing identity verification using deepfakes or synthetic IDs is an immediate material breach.

- **Legal Basis:** Section 5 of the *Cybercrimes Act 19 of 2020* (identity fraud via digital mediums) and common law fraud.

2.7 Data Privacy Violations (POPIA)

Users may not upload documents containing the personal information of third-party data subjects unless explicit, verifiable legal consent or a valid lawful basis under *POPIA* has been established.

- **Legal Basis:** Sections 9–12 of *POPIA*.

3. Monitoring, Detection, and Enforcement

3.1 Detection and Prevention Matrix

The platform deploys a layered technical defense matrix to actively enforce this policy:

Prohibited Action	Real-Time Detection Method	Preventive Operational Measure
Document Forgery	AI pixel-manipulation analysis & metadata validation	Immediate file rejection & system lock
Credential Theft	IP anomaly tracking & behavioral heuristics	MFA prompt / Instant account isolation
Minor Account Creation	Real-time Department of Home Affairs ID verification	Hard gateway block pending Guardian opt-in
Automated Submissions	Network rate-limiting & structural web application firewalls	Advanced CAPTCHA & API key revocation
Certification Tampering	Tamper-evident ledger with cryptographic hash	Dynamic invalidation of the embedded

Prohibited Action	Real-Time Detection Method	Preventive Operational Measure
	chaining; write-once storage	verification QR

3.2 Matrix of Consequences

⚠️ Critical Notice on Violations

Action taken by Oaths.co.za depends on the severity and frequency of the violation. The platform operates on a zero-tolerance framework regarding fraud.

- **Minor Operational Infraction (e.g., uploading unreadable/unsupported document types repeatedly):**
  - *Platform Action:* Written warning followed by temporary 14-day account suspension.
- **Data Protection / POPIA Breach:**
  - *Platform Action:* Immediate deletion of offending data, account suspension, and formal notification to the Information Regulator.
- **Fraud, Forgery, or Identity Deception:**
  - *Platform Action:* Permanent account termination, permanent identity blacklisting, and structural invalidation of all historic digital certificates issued to that profile.
  - *Legal Action:* Mandatory escalation and filing of a criminal case with the South African Police Service (SAPS) Cybercrime Unit and financial reporting to the Financial Intelligence Centre (FIC) where applicable.

4. Legal Text: Prohibited Use Policy

1. General Restrictions

By creating an account, accessing, or utilizing the services provided by Oaths.co.za ("the Platform"), you warrant and agree that you will not utilize the platform for any purpose that:

- Contravenes South African statutory law, common law, or international legal mandates binding on the Republic.
- Aims to perpetrate fraud, misrepresentation, identity theft, or deception.
- Involves the upload, processing, or presentation of altered, forged, or counterfeit documentation.
- Attempts to bypass, trick, or reverse-engineer the biometric facial recognition or identity liveness verification checkpoints.

2. Document and Functional Limitations

The platform is explicitly configured for standard true-copy certification. You agree you will not attempt to submit or process documents requiring alternative legal protocols, including:

- Affidavits requiring physical or unlegislated remote deponent oaths.
- Deeds, wills, or contracts requiring specialized notarization or physical statutory signing elements.
- Documents lacking proper authorization or containing third-party personal data processed in violation of the *Protection of Personal Information Act (POPIA)*.

3. System Security and Integrity

You may not use any automated system, including "robots," "spiders," or "offline readers," to access the Platform in a manner that sends more request messages to the servers than a human can reasonably produce in the same period. You shall not attempt to strip, alter, obscure, or reuse the platform's cryptographic markers, QR verification blocks, or digital validation files on separate or unverified source media.

4. Indemnification

You hereby agree to indemnify, defend, and hold harmless Oaths.co.za, its directors, employees, technology partners, and contracted Commissioners of Oaths against any and all civil claims, damages, statutory penalties, legal costs (calculated on an attorney-and-own-client scale), and losses arising directly or indirectly out of your breach of this Prohibited Use Policy or the submission of fraudulent materials to the platform.

5. Jurisdiction and Governing Law

This Policy is governed strictly in accordance with the laws of the Republic of South Africa. Any legal action, dispute resolution, or enforcement proceedings arising from the violation of these terms shall be subject to the exclusive jurisdiction of the High Court of South Africa (Gauteng Division, Pretoria).
