

POPIA Policy

How we protect personal information under the Protection of Personal Information Act (POPIA).

Version 1.0 · Effective 15 October 2026

Bateleur is the responsible party for learner, guardian, employee and customer information. Children's information, lesson recordings and learning analytics require heightened controls.

Applies to: Directors, employees, educators, contractors, authorised service providers and all systems processing Bateleur information.

Document reference BE-POPIA-001 · Reviewed annually and whenever the law or our practice materially changes.

Purpose, legal framework and reach

This policy establishes mandatory internal controls for processing personal information by Bateleur Education (Pty) Ltd ("Bateleur"), an online education services provider in South Africa. It operationalises the eight conditions for lawful processing in the Protection of Personal Information Act 4 of 2013 (POPIA), read with the Promotion of Access to Information Act 2 of 2000 (PAIA) and applicable regulations.

It applies to applications, enrolment, live online instruction, Moodle and other learning systems, EduCore administration, video-conferencing, recordings, support, accounting, recruitment, third-party integrations, backups and archived records. Each person handling personal information must comply, irrespective of where they work.

Accountability and designated roles

- **Responsible party:** Bateleur determines the purposes and means of its processing and remains accountable for its duties, including work done by operators.
- **Information Officer:** the person holding this role under PAIA/POPIA, ordinarily the head of the private body as defined by law, must oversee compliance, regulator registration where required, privacy requests, training, breach response and recordkeeping. The named officer and deputy details must be maintained in the internal compliance register.
- **System owners and educators:** apply minimum access, confidentiality, safe recording, approved retention and prompt incident escalation. No employee may export learner records to personal storage or unapproved AI tools.
- **Operators:** vendors processing on Bateleur's instructions must be assessed and bound by appropriate written confidentiality and security duties under POPIA section 21, with incident reporting and deletion/return terms.

Lawful collection and processing

- Collect information only for explicit, documented and lawful purposes connected to admission, delivery, learner welfare, reporting, billing, legal duties or otherwise justified processing. Notify individuals of the collection and relevant disclosures when POPIA requires it.
- Identify and record an applicable justification for each activity, such as consent, performance of a contract, legal obligation or a legally permissible legitimate interest. Consent must be voluntary, specific, informed, capable of proof and withdrawable; consent is not the only possible legal basis.
- Minimise data; do not request identity documents, medical details, biometric identifiers or criminal history unless demonstrably necessary and authorised. Keep source, purpose, recipients, safeguards and retention details in a processing inventory.
- Do not reuse learner submissions, recordings or contact details for unrelated publicity, training commercial AI models, advertising or lead generation without a separate lawful basis and appropriate permission.

Children and special personal information

For learners under 18, Bateleur must identify and document a valid POPIA section 35 basis to process the child's information, commonly prior consent from a competent person, or a separate statutory exception. Verify parent/guardian authority proportionately. Give age-appropriate notices and consider the learner's best interests and emerging autonomy.

Medical, disability, safeguarding and other special personal information must be segregated and used only where a POPIA exception and any further applicable requirements permit it, including support arrangements for learners. Disclose on a need-to-know basis, use stricter access controls and do not publish such information.

Advertising profiling and third-party tracking directed at children are prohibited unless independently assessed as lawful, necessary and appropriately authorised; the default position is not to deploy them.

Collection channels and third-party systems

- Approved operational systems may include the Bateleur website, Moodle learning platform, scheduled live video lessons, EduCore learner administration, approved email and payment services. Each supplier must be documented in a current supplier and transfer register.
- Use individual user accounts and role-based access; guardians may access only records they are entitled to receive. Learning analytics and automated outputs must not be treated as conclusive academic, welfare or disciplinary findings without proportionate human review.
- Record classes only when there is a documented educational purpose, suitable notice and lawful authority; restrict access and prohibit unauthorised redistribution or social-media publication.
- Before any cross-border hosting or disclosure, assess POPIA section 72 requirements, destination protections, contract terms and the particular risks to minors.

Security and confidentiality controls

- Require multifactor authentication for privileged accounts where technically available; unique credentials; least privilege; timely leaver access revocation; supported software; patching; malware prevention; encrypted connections and appropriately protected backups.
- Protect exported reports and recordings; restrict downloads and sharing, keep access logs where feasible, and use encryption for portable or highly sensitive records.
- Apply secure vendor onboarding, changes, deletion and incident response. Conduct periodic access reviews, backup restoration tests and staff safeguarding/privacy briefings; document identified control gaps and remediation.
- Never request that a learner sends passwords, banking PINs or one-time passwords by email, WhatsApp or class chat.

Retention, deletion and records of processing

Retain identifiable records only while necessary for the original lawful purpose, authorised compatible purposes or applicable legal/contractual obligations. A documented retention schedule shall specify record owner, trigger date, period, legal justification and secure destruction method; no blanket indefinite retention is authorised.

- **Admissions and academic records:** retain for an evidenced period necessary for learner support, legitimate records requests and applicable obligations. Review annually and securely erase unnecessary duplicates.
- **Finance and tax records:** retain for the period required by applicable tax/accounting legislation; an indicative baseline is at least five years where the relevant statutory rule applies, subject to longer litigation, audit or other obligations.
- **Lesson recordings:** set a published, limited retention period in the enrolment or recording notice; avoid indefinite storage. Safeguarding evidence is preserved under legal hold where necessary.
- Data subject deletion requests are evaluated against legal duties and evidence-preservation requirements; where erasure is not lawful, restrict use and explain the reason.

Data subject rights and complaints

Individuals or their verified authorised representatives may request confirmation of processing, access via the applicable POPIA/PAIA process, correction, deletion where justified, objection where legally available, and withdrawal of consent. Verify identity without collecting excessive replacement information. Respond within statutory timelines and give legally required reasons and review routes.

Submit privacy requests to support@bateleureducation.co.za, marked "POPIA / Information Officer". Complaints may also be directed to the Information Regulator at POPIAComplaints@inforegulator.org.za. Privacy complaints must not lead to learner retaliation.

Security compromises and notifications

Anyone who suspects loss, unauthorised access, ransomware, phishing, accidental disclosure or exposure of a recording must immediately preserve evidence and notify the Information Officer. The incident lead records discovery, scope, risk, containment, affected people, response, recovery and corrective action.

Where reasonable grounds exist to believe that personal information has been accessed or acquired by an unauthorised person, Bateleur must notify the Regulator and affected data subjects as soon as reasonably possible after discovery, subject to POPIA section 22 and any lawful delay. Notification content and channels must satisfy the Act. Do not promise an arbitrary 72-hour deadline as if POPIA imposed one.

Compliance assurance and enforcement

Management reviews supplier compliance, training completion, incidents, the record of processing and changes in law at least annually or after a material event. Breaches of this policy may result in proportionate disciplinary or contractual action, without displacing statutory procedures. The published Privacy Policy explains processing to data subjects; this governance policy defines internal minimum controls.

Legal and operational references

- [Protection of Personal Information Act 4 of 2013, especially ss 11, 18-22, 34-35, 72](#)
- [Information Regulator, POPIA and complaints](#)
- [Information Regulator, complaint contact](#)