

Privacy Policy

Karo Digital Classics Ltd - reading copy. Sign in to Karo to accept and receive your signed copy.

Karo Digital Classics Ltd

Document	Privacy Policy
Issued by	Karo Digital Classics Ltd
Published at	karoschool.net/legal/privacy

KARO PRIVACY POLICY

Version 1.0. Last updated: 13 July 2026. Maintained by Karo Digital Classics Ltd, operator of the Karo school-operations platform, and supported by the standalone Data Processing Agreement and the public Data Protection Impact Assessment.

WHO THIS COVERS

This policy describes how Karo handles information about schools, staff members, students, and guardians whose records the school enters into the platform.

ROLES

Each school is the data controller for the records it enters. Karo Digital Classics Ltd is the data processor and acts only on the school's documented instructions. The controller and processor obligations are set out in full in the standalone Data Processing Agreement which every school owner accepts on first sign-in.

WHAT WE COLLECT

- Account information: full name, phone number, and email for staff logins.
- School records: student and guardian information the School enters.
- Financial records: invoices, receipts, and payment references processed through the platform.
- Operational metadata: login timestamps and audit-log entries so owners can review activity.

We do not process special-category data (health, religion, biometrics) in the ordinary course of business. Payment card and mobile-money credentials are never stored on Karo; those are held by the regulated payment processor.

DATA MINIMISATION FOR PARENTS

Karo collects only what fee collection needs. A guardian's name and phone number are enough to send an invoice, take a payment, and return a receipt. Karo does not ask parents for identity documents, addresses, or income. Parents pay through a regulated payment processor. Card and mobile-money details are never stored on Karo.

HOW WE USE IT

Solely to operate the platform for the school. Karo does not sell information. Karo does not share it with advertisers. Karo does not train third-party AI on it.

SUB-PROCESSORS WE USE

To run the platform we engage the following categories of sub-processor, each bound by a written data-protection agreement no less protective than our DPA:

- Cloud hosting and database - Supabase, hosted on Amazon Web Services in a region approved for the school's data residency.
- Messaging - Meta WhatsApp Business Cloud API (WhatsApp), Africa's Talking Ltd (Nairobi, Kenya - sole SMS carrier for OTPs, invites and delivery notices), Resend (transactional email).
- Payments - Paystack, for card and mobile-money settlement into the school's own bank account.
- PDF generation and delivery - Karo's own document orchestrator and the storage layer above.

Karo notifies schools at least thirty (30) days before adding or changing a sub-processor.

DATA ISOLATION BETWEEN SCHOOLS

Every school's data is sealed in its own tenant. Row-level rules apply to every read and write. A staff member from one school cannot see another school's students, invoices, payments, or reports. Support access follows the same rules and is logged.

ENCRYPTION

All traffic between browsers, phones, and Karo is encrypted in transit. Databases, backups, and file storage are encrypted at rest. Passwords are stored as one-way hashes and are never legible to staff, support, or the platform itself.

ACCOUNT SECURITY

Two-step verification is on for every account. A one-time code is sent to the registered phone at every sign in. Biometric sign-in (face or fingerprint) is available as a fast alternative on the user's own device. Sensitive actions, such as adding or changing a bank account, require a fresh verification code every time.

FINANCIAL RECORD INTEGRITY

Invoices and receipts are permanent once issued. Corrections are made by cancelling and re-issuing, so the original record survives. Every action that touches money is written to an append-only audit trail with the user, timestamp, and change. Auditors can be given a read-only export.

BANK DETAIL PROTECTION

Only the school owner can add or change bank details. Every change requires a password re-entry and a fresh code to the registered phone. New bank accounts sit on an activation hold before they can receive funds. All owners are notified by email each time a bank change is initiated or completed.

RETENTION AND RECOVERY

We apply the maximum lawful retention period to records auditors and courts may need, and a short window to operational detail that does not need to be

kept. These are the windows Karo enforces by scheduled job, not intentions:

- Financial records - invoices, receipts, payments, payment allocations, and the append-only audit log: retained for 7 years from the date each record was created, in line with Kenyan tax and public-audit statutes.
- Academic records - results, report cards, class history: retained, so statements, leaving certificates and historic report cards stay reproducible.
- Message content and delivery records: 45 days by default, configurable by the school in Settings, purged nightly.
- Attendance detail, raw staff clock punches and sick bay visit detail: 90 days, purged nightly. Aggregates are retained.
- Visitor personal data captured at the gate: 45 days, after which the entry is scrubbed to an anonymised audit shell.
- Archived configuration - draft fee structures, unused streams: 30 days after archiving. This purge never touches students, guardians, results, fee profiles, sponsorships, discipline or health records.
- Operational records - students, guardians, staff, message logs, branding assets: retained in a 30-day archive after deletion from the app, from which an owner may restore. After 30 days the archive is purged, unless a legal hold applies.
- DPA and Terms acceptance records: retained for 10 years as legal evidence of the version each user signed under.
- Backups: 30-day rolling schedule; after 30 days the backup is overwritten. Records held for legal reasons persist beyond the archive window. A school may request earlier deletion of its own operational records at any time.

BREACH NOTIFICATION

If Karo confirms a personal-data breach affecting a school's data, we notify that school within 72 hours of confirmation with a written description of the incident, the data affected, and the mitigations taken, so the school can meet its own notification duties under the Act or GDPR.

INTERNATIONAL TRANSFERS

Where personal data is transferred outside Kenya, or outside the European Economic Area for GDPR-subject schools, Karo relies on an adequacy decision, the European Commission's Standard Contractual Clauses (2021/914), or the Office of the Data Protection Commissioner-approved safeguards, whichever apply. A copy of the applicable safeguard is available on request.

YOUR RIGHTS AND PRIVACY REQUESTS

To access, correct, export, or delete personal information held about you, or to raise a privacy question, write to info@karoschool.net. Requests from parents about their own or their children's records are routed to the school that entered the data, since the school is the data controller. Karo assists that school in responding.