

Agreement

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

Karo Digital Classics Ltd

Document	Agreement
Issued by	Karo Digital Classics Ltd
Published at	karoschool.net/legal/agreement

THE KARO AGREEMENT

Version 1.0. Operated by Karo Digital Classics Ltd, Nairobi, Kenya. Safe. Simple. Sorted.

This Agreement is made up of two parts, both of which are accepted together by the signatory named in the signature block of this document:

PART A - Terms of Service: the commercial and operating contract between Karo and the School.

PART B - Data Processing Agreement: the controller-processor terms governing personal data the School entrusts to Karo.

The Karo Privacy Policy is a separate document and is accepted alongside this Agreement at sign-up.

PART A - TERMS OF SERVICE

KARO TERMS OF SERVICE

Version 1.0. Last updated: 9 July 2026. Operated by Karo Digital Classics Ltd, Nairobi, Kenya.

1. PARTIES AND ACCEPTANCE

These Terms form a binding agreement between Karo, operated by Karo Digital Classics Ltd ("Karo", "we", "us"), and the educational institution (the "School") whose administrator creates an account and accepts these Terms on the School's behalf. By ticking the acceptance box during sign up, the person creating the account confirms they are authorised to bind the School.

2. THE SERVICE

Karo is a school fees management platform. Karo helps the School record students and guardians, publish fee structures, generate invoices, receive payments, reconcile receipts, communicate with parents, and produce reports. Karo does not provide legal, tax, or accounting advice.

3. ROLES AND DATA OWNERSHIP

The School is the data controller of all student, guardian, staff, and financial information it enters into Karo. Karo is a data processor acting solely on the School's instructions to operate the service. All records the School creates in Karo remain the property of the School and can be exported at any time.

4. ACCOUNT SECURITY AND DELEGATION

The School is responsible for all activity performed under its account. Each staff member must sign in with their own credentials. Two-factor authentication is required. The School is expected to revoke access promptly when staff leave and to use Karo's role settings to delegate only the access each role requires.

4A. PLATFORM SECURITY COMMITMENTS

Karo maintains the following protections for every school on the platform. Traffic is encrypted in transit. Databases, backups, and file storage are encrypted at rest. Passwords are stored as one-way hashes. Two-step verification is on for every account, with a code to the registered phone at each sign in and optional biometric sign-in on the user's own device. Each school's data is sealed in its own tenant with row-level rules on every read and write. Invoices and

receipts are permanent once issued and every money-touching action is written to an append-only audit trail. Bank account changes require re-authentication, sit on an activation hold, and trigger owner alerts. Deleted records enter a 30-day archive so an owner can restore an accidental deletion before it is purged.

5. FEES

Karo's platform fee is KES 299 per student per term. The fee is recovered at source: as invoiced fees for a student are paid, the platform fee for that student and term is deducted from the first collections until fully recovered, and the balance settles to the School. There is no setup fee, no monthly minimum, and no charge for students against whom no payment is collected.

6. PAYMENTS AND SETTLEMENT

All parent payments are collected through Karo's regulated payment processor and settle directly to the School's registered bank account, minus the platform fee described above. Karo does not hold School funds at any point. The School is responsible for the accuracy of the bank account details it registers for settlement and for reconciling settlement statements with its own records.

7. MESSAGING CONDUCT

Karo may send messages to guardians on the School's behalf strictly for legitimate fees and school-parent communication. The School must not use Karo to send unsolicited marketing, political messaging, or content unrelated to the School's relationship with the guardian.

7A. AML / KYC POSTURE

Karo is a software service. Karo does not hold, pool, or transmit school funds; fees are collected and settled by a licensed payment service provider directly to the School's own bank account. The School is responsible for its own anti-money-laundering, tax, and know-your-customer obligations toward its guardians and regulators.

8. SERVICE AVAILABILITY

Karo aims for continuous availability of the service but does not guarantee it will be uninterrupted or error free. Karo may perform scheduled maintenance and will make reasonable efforts to give advance notice for changes that affect School operations.

9. SUSPENSION AND TERMINATION

The School may terminate its account at any time from the settings screen or by writing to us. Karo may suspend or terminate access if the School breaches these Terms, fails to pay platform fees due, or uses the service in a manner that endangers other users or third parties. Immutable financial records (issued invoices, receipts, and audit log entries) are retained for the period required by applicable law and remain exportable by the School during that period.

10. LIABILITY

To the maximum extent permitted by law, Karo's aggregate liability under this agreement is limited to the platform fees paid by the School in the twelve months preceding the event giving rise to the claim. Karo is not liable for indirect, incidental, or consequential losses, including loss of profit, goodwill, or data not caused by Karo's gross negligence.

11. GOVERNING LAW

These Terms are governed by the laws of the Republic of Kenya. Any dispute arising from or in connection with these Terms shall be submitted to the exclusive jurisdiction of the courts of Kenya.

12. CHANGES TO THESE TERMS

Karo may update these Terms. Material changes are versioned; when the version changes, the School's next authorised administrator sign in prompts a fresh acceptance before continued use.

13. CONTACT

All questions about these Terms, notices, and support requests: info@karoschool.net

PART B - DATA PROCESSING AGREEMENT

DATA PROCESSING AGREEMENT (Version 1.0)

This Data Processing Agreement ("DPA") forms part of the agreement between:

- (A) The school, college, university, or other education institution identified in the Karo account of the accepting user ("Controller"), represented by the signatory below; and
- (B) Karo Digital Classics Ltd, a company incorporated in the Republic of Kenya and registered or in the process of registering to operate in other East African Community member states, operator of the Karo school-operations platform ("Processor", "Karo").

together the "Parties". Karo processes personal data on the Controller's behalf as its processor within the meaning of the data protection law applicable to the Controller's place of establishment (the "Applicable Data Protection Law"), and, where applicable to the Controller, Article 28 of the EU General Data Protection Regulation (Regulation (EU) 2016/679, "GDPR").

APPLICABLE DATA PROTECTION LAW AND MULTI-JURISDICTION SCOPE

Karo operates across East Africa. Where the Controller is established in, or processes the personal data of data subjects located in, a country listed below, the corresponding statute and supervisory authority apply to this DPA in addition to (and, where stricter, in priority over) the general terms here:

- (a) Kenya - Data Protection Act, 2019; Office of the Data Protection Commissioner.
- (b) Uganda - Data Protection and Privacy Act, 2019; Personal Data Protection Office.
- (c) Tanzania - Personal Data Protection Act, 2022; Personal Data Protection Commission.
- (d) Rwanda - Law No. 058/2021 relating to the protection of personal data and privacy; National Cyber Security Authority.
- (e) Any other jurisdiction in which Karo is lawfully registered to provide the platform at the time of processing, whose national data protection statute and supervisory authority will then apply on the same basis.

Karo will register with, notify, or license itself before each competent supervisory authority to the extent the Applicable Data Protection Law requires this of a processor, and will maintain records of processing in the form that law prescribes. Nothing in this DPA reduces a data subject's rights or a Controller's obligations under the law of the Controller's own country.

1. SUBJECT MATTER AND DURATION

Karo processes personal data solely to provide the Karo platform to the Controller: enrolling students and guardians, issuing invoices, collecting payments through regulated payment processors, delivering receipts and notices, and producing operational reports. This DPA applies for as long as the Controller's Karo account is active and, for retention purposes, for the periods set out below.

2. CATEGORIES OF DATA SUBJECTS AND PERSONAL DATA

Data subjects: staff members, students, and guardians of students. Categories of personal data: full names, phone numbers, email addresses, admission numbers, class and stream assignments, guardian relationships, invoice line items, payment references, receipt numbers, message delivery status, and login/audit metadata. Karo does not process special-category data (health, religion, political opinion, biometrics) as a normal course of business. Card and mobile- money credentials are never stored on Karo; those are held by the regulated payment processor.

3. ROLES

The Controller determines the purposes and means of processing and is solely responsible for the lawful basis of every record it enters into Karo. Karo processes personal data only on the Controller's documented instructions, which for standard operations are the configurations and actions performed through the Karo application. Additional instructions must be given in writing to info@karoschool.net.

4. PROCESSOR OBLIGATIONS

Karo will:

- (a) process personal data only on the Controller's instructions and only for the platform's operating purposes;
- (b) ensure every person authorised to access personal data is bound by a written duty of confidentiality;
- (c) implement and maintain the technical and organisational security measures described in Schedule A below;
- (d) assist the Controller in responding to data-subject rights requests (access, rectification, erasure, restriction, portability, objection) within the timelines that apply to the

Controller under the Act or GDPR;

- (e) notify the Controller without undue delay, and no later than seventy-two (72) hours after becoming aware, of any personal-data breach affecting the Controller's data;
- (f) at the Controller's choice, delete or return all personal data at the end of the service, subject to the retention periods in clause 8; and
- (g) make available all information reasonably necessary to demonstrate compliance with this DPA and permit audits carried out by the Controller or an independent auditor mandated by the Controller, at reasonable intervals, on reasonable notice, and subject to appropriate confidentiality undertakings.

5. CONTROLLER OBLIGATIONS

The Controller warrants that it has a lawful basis to process the personal data it enters into Karo, has provided any notices required under the Act or GDPR to its data subjects, and will not upload personal data of any child except in the ordinary course of school administration.

6. CONFIDENTIALITY AND NON-DISCLOSURE

Each Party may receive or access non-public information from the other Party in connection with setting up, operating, evaluating, supporting, auditing, or improving a Karo account ("Confidential Information"). Confidential Information includes, without limitation: platform source code, database schemas, API keys, integration credentials, security controls, product roadmaps, pricing arrangements, user lists, message templates, fee structures, student and guardian data, payment settlement details, banking configuration, school operational records, and any information marked or reasonably understood as confidential.

Each Party will: (a) hold the other Party's Confidential Information in strict confidence; (b) use it only for the purposes of using, providing, supporting, securing, or evaluating Karo; (c) protect it with at least the same degree of care it uses for its own confidential information, and never less than reasonable care; (d) disclose it only to employees, contractors, sub-processors, or professional advisers who need to know it and are bound by equivalent confidentiality duties; (e) not reproduce, reverse-engineer, decompile, attempt to derive source code from, copy, benchmark publicly, or replicate any Karo software or infrastructure; and (f) not use Confidential Information to compete with, undermine, or harm the other Party's business, staff, schools, guardians, students, or suppliers.

These obligations do not apply to information that is publicly known through no breach of this DPA, already lawfully possessed without a duty of confidentiality, independently developed without reference to the other Party's Confidential Information, or required to be disclosed by law or a competent authority, provided the receiving Party gives prompt written notice where lawful. No license, ownership, or intellectual-property right is granted by disclosure. All Karo software, brand assets, documentation, templates, and derivative works remain the property of Karo Digital Classics Ltd.

Confidentiality obligations apply for the duration of the Controller's Karo account and for 10 years thereafter.

Obligations relating to personal data, trade secrets, source code, security controls, credentials, and banking or payment configuration survive for as long as the information remains legally protectable or confidential. The Parties acknowledge that breach may cause irreparable harm, and the non-breaching Party may seek injunctive relief in addition to any other remedy available at law or equity.

7. SUB-PROCESSORS

The Controller authorises Karo to engage the following categories of sub-processors:

- (i) cloud hosting and database (Supabase, hosted on Amazon Web Services within a region approved for the Controller's data residency);
- (ii) transactional messaging carriers (Meta Platforms Ireland Ltd via the WhatsApp Business Cloud API for WhatsApp; Africa's Talking Ltd, Watermark Business Park, Ndege Road, Karen, P.O. Box 15310-00100 Nairobi, Kenya, as the sole SMS carrier for OTPs, invite links, delivery status and staff notifications, processing recipient phone number, message content and delivery timestamps, with delivery metadata retained by the carrier under its own schedule and the message body retained in Karo's own message_log for the in-life window in clause 9(e); Resend for transactional email);
- (iii) payment processing (Paystack for card and mobile-money settlement to the Controller's own bank account);
- (iv) document generation and delivery (Karo's own PDF orchestrator and the storage layer above).

Karo will impose data-protection obligations on each sub-processor that are no less protective than this DPA. Karo will notify the Controller of any intended change of, or addition to, sub-processors at least thirty (30) days in advance and

give the Controller the opportunity to object on reasonable data-protection grounds.

8. INTERNATIONAL AND CROSS-BORDER TRANSFERS

Karo hosts and processes personal data in cloud regions selected for the Controller's data residency requirements, and may process data across East African Community member states in which it is registered in order to provide, support and secure the platform. Where personal data is transferred out of the country in which the Controller is established, or, for GDPR-subject Controllers, outside the European Economic Area, Karo will rely on whichever of the following applies under the Applicable Data Protection Law: an adequacy or equivalence decision; the standard contractual clauses issued by the European Commission (2021/914); safeguards approved or registered with the competent supervisory authority (including the Kenyan Office of the Data Protection Commissioner, the Ugandan Personal Data Protection Office, the Tanzanian Personal Data Protection Commission, or the Rwandan National Cyber Security Authority); or the Controller's own explicit authorisation where the law permits it. Where a national law requires a copy of records to remain within that country, Karo will keep a resident copy in that country. A copy of the applicable safeguard is available on request.

9. RETENTION

Karo retains personal data for as long as the Controller's account is active. On termination:

- (a) Financial records, invoices, receipts, payments, payment allocations, and the append-only audit log, are retained for 7 years from the date each record was created, or the longer period required by the tax and public-audit statutes of the Controller's own country. This reflects the retention required by East African tax and public-audit statutes and is applied so records remain available to auditors and to the Controller for the full lawful period.
- (b) Operational records, students, guardians, staff, message logs, branding assets, are retained in a thirty (30) day archive from which the Controller may restore, then purged, unless the Controller requests earlier deletion or a legal hold applies.
- (c) DPA and Terms acceptance records are retained for 10 years for compliance evidence.
- (d) Backups follow their own thirty (30) day rolling schedule and are then overwritten.
- (e) While the account is active, Karo additionally enforces shorter in-life windows by scheduled job, and these run whether or not the account is terminated: message content and delivery records are purged after forty-five (45) days by default, a window the Controller may change in Settings; attendance detail, raw staff clock punches and sick bay visit detail are purged after ninety (90) days, with aggregates retained; visitor personal data captured at the gate is scrubbed after forty-five (45) days, leaving an anonymised audit shell; archived configuration is purged thirty (30) days after archiving without touching students, guardians, results, fee profiles, sponsorships, discipline or health records. Records in clause 9(a) are never purged on a schedule.

10. DATA-SUBJECT REQUESTS

If Karo receives a request from a data subject relating to personal data processed on the Controller's behalf, Karo will (a) not respond substantively other than to acknowledge receipt and route the request to the Controller, and (b) provide the Controller with reasonable assistance to respond within its statutory time limits.

11. LIABILITY AND INDEMNITY

The Parties' liability under this DPA is subject to the limits set out in the Karo Terms of Service. Neither Party excludes liability that cannot lawfully be excluded, including liability under the Act for breaches attributable to that Party.

12. GOVERNING LAW AND JURISDICTION

This DPA is governed by the laws of the Republic of Kenya, save that where the Controller is established outside Kenya, the mandatory provisions of the Applicable Data Protection Law of the Controller's country prevail over this DPA to the extent of any conflict, and the competent supervisory authority and courts of that country retain jurisdiction over matters those provisions reserve to them. Subject to that, the courts of Nairobi have jurisdiction, without prejudice to either Party's right to seek interim relief in any competent jurisdiction, and to any mandatory right of a data subject under the Applicable Data Protection Law or GDPR to bring proceedings in the courts of their habitual residence.

13. ORDER OF PRECEDENCE

In case of conflict, this DPA prevails over the Karo Terms of Service to the extent of the conflict on data-protection matters, followed by the Terms of Service, followed by any Karo policy published on karoschool.net.

SCHEDULE A, TECHNICAL AND ORGANISATIONAL MEASURES

- A1. Encryption
All traffic between browsers, phones, and Karo is encrypted in transit using industry-standard TLS. Databases, backups, and file storage are encrypted at rest. Passwords are stored as one-way hashes.
- A2. Access control
Access to the platform is restricted through per-tenant row-level security. Two-step verification is mandatory for every account. Sensitive actions (adding a bank account, exporting data, impersonation by platform support) require a fresh one-time code and are written to an immutable audit trail.
- A3. Tenant isolation
Each 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 read another school's records.
- A4. Financial record integrity
Invoices and receipts are permanent once issued; corrections are made by cancellation and re-issue so the original record survives. Every action that touches money is written to an append-only audit log with actor, timestamp, and delta.
- A5. Incident response
Karo maintains a documented incident-response procedure. Suspected personal-data breaches are triaged within twenty-four (24) hours and notified to the Controller within seventy-two (72) hours of confirmation, together with a written description of the incident, the data affected, and mitigations taken.
- A6. Sub-processor management
Sub-processors are subject to written data-protection agreements at least as protective as this DPA and are reviewed at least annually.
- A7. Data-subject request tooling
Access, rectification, and export operations are available to the Controller through the Karo platform. Erasure and portability requests are supported by the Karo support team on written instruction from the Controller.

ACCEPTANCE

By checking the acceptance box and submitting your full name, your role at the Controller institution, and the Controller's legal name, You confirm that You are authorised to bind the Controller to this DPA, including its confidentiality and non-disclosure obligations, on the Controller's behalf. You confirm that You have read, understood, and agreed to it. Your typed full name constitutes your electronic signature under applicable law.

Contact: info@karoschool.net

=====
END OF THE KARO AGREEMENT
=====