KARO *Safe. Simple. Sorted.*

Published copy

Data Protection Impact Assessment

Karo Digital Classics Ltd - issued and in force. Published copy.

Karo Digital Classics Ltd

Document	Data Protection Impact Assessment
Issued by	Karo Digital Classics Ltd
Published at	karoschool.net/legal/dpia

1. Purpose and scope

This assessment answers one question honestly: does running a school on Karo put children, their families or school staff at a risk that is not properly controlled. It is written for a school's board, a school's lawyer and a supervisory authority, and it is deliberately specific about what is not yet solved.

Karo is an education-operations platform for institutions across Africa: primary and secondary schools, international and comprehensive schools, colleges and universities. It records enrolment, fees and payments, attendance, examinations and report cards, transport, visitor and gate movements, sick bay visits, discipline, staff time and staff leave, and it sends operational messages to guardians over WhatsApp and email. Karo operates across the continent, with Kenya as the jurisdiction of incorporation and the primary operating jurisdiction. This assessment is written against the Kenya Data Protection Act 2019 as the operating standard, applied consistently wherever an institution is based, and is reviewed against local law before the first institution in a new jurisdiction goes live.

The assessment at a glance

Field	Position
Assessed system	The hosted Karo platform, all modules, web and installed app
Market served	Primary and secondary schools, international and comprehensive schools, colleges and universities across Africa
Footprint	Operating across Africa, with Kenya as the jurisdiction of incorporation and primary operating jurisdiction
Out of scope	An institution's own offline records, its other systems, and anything it exports and then handles itself
Operator	Karo Digital Classics Ltd, processor
Controllers	Each subscribing school, for the records it enters
Data subjects	Children, guardians, school staff, gate visitors, the school's signatory
Why an assessment is required	Large-scale processing of children's data, health data about minors, biometric-adjacent identity documents, and systematic monitoring of movement on site. Kenya Data Protection Act 2019 section 31 and the Data Protection (General) Regulations 2021, equivalent to GDPR Article 35
Assessment status	**Issued and in force. Filed on Karo's data protection record and published to subscribing institutions**
Review cadence	At least annually, and on any change to processors, data categories or purposes

2. Roles and lawful basis

Party	Role	Lawful bases relied on

Document hash (SHA-256): b6407931de31cbeda91a46e008f494a20026e6db8cfbcdadd4e0342bf4facc65

Party	Role	Lawful bases relied on
Subscribing school	Controller	Contract with the family (enrolment, fees, results); legal obligation (tax and audit retention, safeguarding duties); legitimate interests in the safety of children on site (attendance, gate, transport); vital interests and explicit consent for health data
Karo Digital Classics Ltd	Processor, on documented instruction	Part B (Data Processing Agreement) of the Agreement, accepted by the school's authorised signatory on first sign-in
Karo Digital Classics Ltd	Controller, for its own narrow processing	Contract performance and its own legal obligations: account creation, signatory identity verification, billing, platform security and fraud prevention

Health information and identity documents are treated as sensitive personal data throughout, with the narrower bases above and the tighter controls in section 6.

3. Data categories actually processed

Verified against the live schema, 155 tables in the application schema.

Category	What is held	Sensitivity
Children	Name, admission number, date of birth, sex, class, stream and class history, photograph, subject choices, marks at component level, aggregated results and positions, report cards, attendance, transport route and stop, authorised pickup persons, fee profile, invoices, payments, receipts, statements, sponsorships, exit status and leaving documents	**High, minors**
Children's health	Health profile (conditions, allergies, medication, emergency instructions) and sick bay visits	**Highest**
Guardians	Name, relationship, up to two numbers per child, email, WhatsApp and channel preference, consent records, message history, payment history, meeting bookings	**Medium**
Staff	Name, role, contact, invitation and join records, passkey credentials and phone, clock events with geolocation against a defined zone, leave and balances, cover assignments, permission scopes, signature images	**Medium to high**
Gate visitors	Name, phone, identity capture, party members, vehicle plate, carrier contact, host and purpose, item and pickup passes	**Medium**
School signatory	Name, role, identity document number and image, phone, email, registration and bank verification documents for payout setup	**High**
Payments	Invoice and receipt detail, amounts, channel, provider reference, allocation, refunds, manual payment approvals, platform fee ledger	**Medium**
Platform and security	Append-only audit log, message delivery log, passcode dispatch log, push subscriptions, impersonation log, portal login attempts	**Medium**

4. Data flows, processors and change notification

Verified from the outbound integrations present in the codebase. This table lists the processors that handle live school data today, and is the published sub-processor list, also available at karoschool.net/legal/sub-processors, last updated 17 August 2026.

Processor	Purpose	Data received	Status
Lovable Cloud (Supabase infrastructure)	Hosting, database, authentication, file storage, backups	All categories in section 3, at rest	**Live, European Union**
Africa's Talking	WhatsApp and message delivery	Recipient phone number, message body, document link	**Live, Kenya**

Processor	Purpose	Data received	Status
Paystack	Payment collection and settlement to the school	Payer name, email or phone, amount, school subaccount reference	**Live, Nigeria and South Africa**
Mailgun (via Lovable email infrastructure)	Transactional email delivery	Recipient email, subject, rendered body, document link	**Live, European Union and United States**
Cloudflare	Edge delivery and bot protection (Turnstile) on sign-up	Requesting IP address and challenge token. No school records	**Live, Global edge**
GoDaddy	Domain registration and DNS for karoschool.net	No school or guardian records. Karo's own registrant and billing details only, plus DNS lookups	**Live, United States**

Change notification commitment. Karo will give every subscribing school at least 30 days' written notice, by email to the school's registered contact and by an update to this page, before a new sub-processor begins processing school data, and before an existing one is replaced. A school that objects on reasonable data-protection grounds may raise the objection within that notice period; if the objection cannot be resolved, the school may terminate the affected service without penalty for the remainder of the paid period. Emergency substitutions to keep the service running are notified within 5 days of the change, with the same objection right.

Verification of the person signing for the institution is manual. A member of Karo's team compares the uploaded National ID, passport or driving licence with the details given, by eye, on the admin console, and approves or asks for a replacement. There is no automated facial matching, liveness scoring or automated approval anywhere in that flow. One-time passcodes are generated and checked by Karo's own store and delivered through the messaging processor above or by email.

Documents (receipts, statements, report cards) are delivered to families as tokenised links, never as attachments or generated images, so document content does not transit the messaging processor.

5. Retention, as enforced by Karo

Data	Window	Enforced by
Financial records and audit log	7 years minimum	Never deleted on a schedule. Committed floor matching Kenyan tax and audit requirements
Academic records, results, class history	Retained	Kept so statements, leaving certificates and historic report cards stay reproducible
Archived configuration (draft fee structures, unused streams)	30 days after archiving	Daily job public.purge_expired_archives. It explicitly does not touch students or guardians
Attendance and staff clock detail	90 days for detail	Scheduled purge, aggregate retained
Sick bay visit detail	90 days	Scheduled purge
Visitor personal data at the gate	45 days	Scheduled scrub, leaving an anonymised audit shell
Message content and delivery records	45 days by default	School-configurable window, scheduled purge
Single learner's operational history, on request	On demand	public.purge_student_history. Requires an owner or administrator, an exact typed confirmation of the learner's name, a written reason of at least ten characters, and it writes an audit entry. Removes attendance, sick bay, gate passes, discipline and health. Does not remove financial or academic records

These windows are the minimum baseline Karo enforces, not a ceiling a school is locked into. A subscribing school may ask Karo at any time to review its retention arrangements, and where a shorter window, a longer window or a different treatment of a category is required by the school's own policy or by its regulator, that is agreed in writing and configured for that school.

The non-cascade guarantee is load-bearing: purges of archived configuration never touch students, guardians, results, fee profiles, sponsorships, discipline or health records, and that boundary is pinned by regression tests.

6. Access controls in place

Control	How it works
Tenant isolation	Row-level security on all 155 application tables with 313 policies. Every record is scoped by school identifier; there is no route by which one school reads another's data
Roster visibility	Class teachers see their own classes, senior leadership sees the school. This replaced a broader read that exposed the full roster to any signed-in member
Health records	Gated separately from the general student record; every read and write is written to the append-only audit log by a database trigger, so access is attributable after the fact
Guardian consent	Captured explicitly as first-class records, consent requests and recorded consents, never inferred
Authentication	Passkey and device biometric first, one-time passcode fallback. The biometric is the device's own WebAuthn factor; no facial image or biometric template reaches Karo
Privileged access	Karo console access is role-gated and IP-allowlisted, impersonation is logged and swept
Idle sessions	**Five minutes of genuine inactivity signs the session out server-side. Returning requires fresh credentials, which establishes a new session rather than resuming the old one**
Public document links	192 bits of token entropy, rate limited, rendered in a view-only viewer

7. Security controls and practices in place

These are standing practices, run continuously rather than as a one-off exercise. Findings from them are fixed and, where they change the risk picture, carried into sections 8 and 9.

Practice	What it means in operation	Cadence
Tenant-scoping review	Every server function and query path is reviewed for school scoping, and automated cross-tenant tests fail the build if a path can read another school's records	**Every change**
Row-level security linting	Automated checks flag any table without row-level security or without a policy, and any policy that widens access beyond the intended role	**Continuous**
Least-privilege review of read paths	Student, health and financial read paths are scoped to the role that needs them, class teachers to their classes and senior leadership to the school, rather than to any signed-in member	**Continuous**
Regression pinning of safety behaviours	Behaviours that protect data (non-cascading purges, link-only document delivery, health access logging) are pinned by tests, so a regression fails the build rather than reaching a school	**Every build**
Access attribution	Health record access, privileged console access and impersonation are written to an append-only audit log, reviewed when anything looks anomalous	**Continuous**
Dependency and platform scanning	Automated dependency and security scanning of the running platform, with findings triaged and fixed	**Continuous**
Platform security assessment	Structured assessment of access control, tenant isolation, data flows, retention and supply chain across all modules, carried out by Classic Talent Optimization (an affiliated party, not an independent assessor). Published in full at karoschool.net/legal/security-assessment	**Completed, published**
Rehearsed incident response	Tabletop incident exercise run against the section 12 outline, with date, participants, scenario and findings recorded at karoschool.net/legal/incident-drill	**At least annually**

8. Risk assessment and residual risk

Impact is stated as impact on the data subject. Residual risk is after the mitigations in sections 5, 6 and 9. Green means accepted as low, amber means live and monitored, red means unacceptable and blocking.

Risk	Impact	Mitigations	Residual

Document hash (SHA-256): b6407931de31cbeda91a46e008f494a20026e6db8cfbcdadd4e0342bf4facc65

Risk	Impact	Mitigations	Residual
Unauthorised disclosure of a child's health data	High	Separate policy, trigger-based audit of every access, 90-day purge of detail, five-minute session termination limits an unattended device	Amber
Cross-tenant data leakage	High	Row-level security on every table, school-scoped server functions, automated cross-tenant tests that fail the build	Green
Message sent to the wrong guardian	Medium	Per-child guardian records with explicit channel preference, delivery logging, delivery centre showing failures and allowing corrected resends	Amber
Compromise of a staff device or account	High	Passkey and biometric primary authentication, full session termination after five minutes of inactivity, scoped permissions, audit log	Green
Payment fraud or misdirected settlement	High	Bank verification documents reviewed before go-live, maker-checker approval on manual payments and refunds, reconciliation against the provider every 30 minutes, discrepancy digest	Green
Processor failure or breach at a third party	Varies	Minimum necessary data per processor, no card data held, no child biometrics sent anywhere, documents delivered as tokenised links, published sub-processor list with notice period	Amber
Excessive retention	Medium	Enforced windows in section 5 and the explicit non-cascade guarantee	Green
Accidental irreversible deletion	High	Retention contract, typed confirmation and audit on the deliberate purge path, documented restore request path in section 10	Green
Rights request not answered in time	Medium	Self-service intake at /privacy-request, console queue with a response clock, acknowledgement and fulfilment targets in section 11	Green
Undetected weakness in the platform itself	High	Completed platform security assessment with findings closed and regression-tested, plus continuous regression tests, RLS linting and dependency scanning. The assessor is internal and affiliated rather than independent, see section 9	Green

The remaining amber lines are honest, not pending paperwork. Health data stays amber because a legitimately authorised staff account can read what it is entitled to read, and no technical control fixes that; detection and attribution are the answer. Wrong-guardian messaging stays amber because the accuracy of the number is the institution's own data entry. Third-party breach stays amber because it is partly outside Karo's control.

9. Data protection controls and assurance

The controls below are implemented and running in the platform today. Nothing appears here as intention.

Control	What is in place	Status
Session termination on inactivity	Five minutes of genuine inactivity ends the session server-side. Returning requires a passkey, a device biometric prompt or a fresh passcode, and issues a new session rather than resuming the old one. An unattended device does not stay signed in	In place
Data subject request handling	Anyone may lodge an access, correction, objection or erasure request at karoschool.net/privacy-request. Each request enters a tracked queue with a response clock: acknowledged within 3 days, substantive response within 30 days, as set out in section 11	In place
Documented restore request path	A published, step-by-step route for a school to request recovery of lost records, with named acknowledgement and restore targets and a written audit trail. Section 10	In place
Published sub-processor list with change notification	Every processor handling live school data is listed in section 4 and at karoschool.net/legal/sub-processors, with 30 days' written notice before any addition or replacement and a right to object	In place

Document hash (SHA-256): b6407931de31cbeda91a46e008f494a20026e6db8cfbcdadd4e0342bf4facc65

Control	What is in place	Status
Retention enforced, with a school-requestable review	The windows in section 5 are enforced by scheduled jobs, not by policy alone, and a subscribing school may ask at any time for its retention arrangements to be reviewed and configured to its own policy or regulator	**In place**
Rehearsed incident response	A tabletop exercise against the section 12 outline, recorded with date, participants, scenario and findings, repeated at least annually and published at https://karoschool.net/legal/incident-drill	**In place**
Platform security assessment	A structured assessment of access control, tenant isolation, data flows, retention and supply chain across all modules, carried out by Classic Talent Optimization, an internal and affiliated assessor rather than an independent one. Findings closed and regression-tested. Published in full at https://karoschool.net/legal/security-assessment	**In place, affiliated assessor**

An independent third-party security assessment has not yet been completed; one is being commissioned ahead of scaling beyond the current pilot schools, and its result will be published here alongside the assessment above.

Assurance reports on file. Two reports sit behind this section and may be read in full by any subscribing institution, its lawyer or a supervisory authority.

Report	Scope, author and date	Where to read it
Platform Security Assessment	Access control, tenant isolation, data flows, retention and supply chain across all modules. Carried out by Classic Talent Optimization, an affiliated assessor, dated 15 August 2026. Findings closed and regression-tested, with no unresolved finding known at the date of the report	https://karoschool.net/legal/security-assessm
Incident Response Drill Record	Tabletop exercise against the incident response outline in section 12, run by Classic Talent Optimization, an affiliated party, dated 15 August 2026, recorded with participants, scenario and findings, repeated at least annually	https://karoschool.net/legal/incident-drill

Both reports are published view-only under the same access pattern as the Agreement and the Privacy Policy. They are assurance work by an affiliated party; they are not certification by a supervisory authority and are not presented as such.

10. Restore request path

Backups are taken at the hosting layer with point-in-time coverage. A school cannot restore itself; it asks Karo, and Karo restores on the school's written instruction. This is the documented path.

Step	What happens	Target
1	The school owner or an administrator emails info@karoschool.net from the registered school contact, stating what was lost, roughly when, and the last time it was known to be correct	Any time
2	Karo acknowledges and confirms the identity of the requester	**Within 1 business day**
3	Karo assesses whether the data can be recovered from the retention windows in section 5, from the audit log, or from a point-in-time backup, and tells the school which	**Within 2 business days**
4	On written approval from the school, Karo performs a scoped restore of the affected records and reports what was and was not recovered	**Within 5 business days of approval**
5	The request, the approval and the outcome are written to the audit log	Same day

Limits stated plainly: a restore may reintroduce records the school deliberately deleted in the same window, so scope is agreed in writing first.

Document hash (SHA-256): b6407931de31cbeda91a46e008f494a20026e6db8cfbcdadd4e0342bf4facc65

Data already purged by a published retention window in section 5 is gone and cannot be restored.
A restore never crosses schools. Only the requesting school's records are touched.

11. Data subject rights, what is supported today

Right	Supported	How it works
Access	Yes	A guardian can view and download the child's receipts, statements over any period within the retention window, and published report cards, through tokenised view-and-download links. A written request can be made at /privacy-request
Rectification	Yes	The school corrects any record it entered; corrections to student, fee and guardian records are audited
Objection to messaging	Yes	WhatsApp and channel preferences can be turned off per guardian, and email carries one-click unsubscribe
Erasure of operational history	Yes	The audited single-learner purge in section 5, exercised by the school
Portability	Yes	CSV and PDF export across modules, in practical rather than machine-negotiated form
Request intake and response clock	Yes	Public form at /privacy-request, acknowledged within 3 days, substantive response within 30 days as required by the Act, tracked in the Karo console queue
Erasure of financial or academic records inside the statutory period	No, and not claimed	Retained for 7 years as a legal obligation. Neither a school nor Karo can override this in the product

12. Breach response outline

Detection through platform logging, the append-only audit log, delivery and reconciliation monitoring, and reports to info@karoschool.net.

Stage	Action	Timing
Contain	Revoke affected access, isolate the path, stop the bleeding	Immediately
Assess	Scope the exposure from the audit log and delivery records	Within 24 hours
Notify the school	Tell the affected school as controller, with the facts known at that point	Within 48 hours of confirmation
Support regulator notification	Help the school notify the Office of the Data Protection Commissioner where the threshold is met	Within 72 hours
Record	Incident, remediation and the preventive change, recorded on the incident register	On closure

This outline has been rehearsed. The drill record, with date, participants, scenario and findings, is published at https://karoschool.net/legal/incident-drill.

13. Owner, contact and status

Karo Digital Classics Ltd, operator of the Karo school-operations platform. Data protection contact: info@karoschool.net. Reviewed at least annually, and on any material change to processing, processors, or the categories of data collected.

STATUS. This assessment is issued and in force. It is filed on Karo's data protection record, published to subscribing institutions, and read alongside the Platform Security Assessment and the Incident Response Drill Record. It is not a certification issued by a supervisory authority or by an independent assessor, and should not be presented as one.

Document hash (SHA-256): b6407931de31cbeda91a46e008f494a20026e6db8cfbcdadd4e0342bf4facc65