Renode LMS Platform Privacy Policy

Effective date: 24 May 2026
Responsible party: Renode Technologies (Pty) Ltd
Platform: Renode LMS Platform / OpenCampus LMS
Contact: info@renode.co.za

Executive Summary

This Privacy Policy explains how Renode Technologies (Pty) Ltd processes personal information through the Renode LMS Platform. The platform is used by schools, tertiary institutions, skills development providers, enterprise academies, sponsors, learners, teachers, administrators and LMS provider staff.

Renode Technologies is committed to lawful, fair, transparent and secure processing of personal information in accordance with the Protection of Personal Information Act, 2013 (POPIA), the South African Children's Act, 2005, the General Data Protection Regulation (GDPR), the California Consumer Privacy Act as amended by the California Privacy Rights Act (CCPA/CPRA), and generally accepted child online protection principles.

This policy is written for institutional customers, learners, parents, guardians, sponsors, employees, contractors, regulators and enterprise reviewers.

Scope

This policy applies to:

- Visitors to the Renode LMS public website.
- Institutional customers using the LMS as a white-label platform.
- Admin users, teacher users, learner users, sponsor users and LMS provider users.
- Demo request submitters.
- Support ticket requestors.
- Users whose personal information is processed through integrations such as payment providers, online meeting providers, SSO providers and cloud infrastructure providers.

Roles Under Privacy Law

Party	Typical Role
Institution customer	Responsible party/controller for its learners, teachers, sponsors and academic records.
Renode Technologies	Operator/processor for institution data and responsible party/controller for its own website, provider portal, support and commercial records.
Learner, teacher, sponsor, admin or visitor	Data subject.
Payment, hosting, storage, email and meeting providers	Operators/processors or independent controllers depending on service context.

Information Collected

Account and Identity Information

The platform may process names, surnames, usernames, email addresses, phone numbers, job titles, roles, institution identifiers, profile pictures, language preferences and account status.

Learner and Education Information

The platform may process enrolment records, course progress, assessment answers, grades, submissions, attendance-related class participation, discussion posts, comments, messages, calendar entries and learning activity data.

Child Personal Information

Where learners are children, the platform may process child personal information on behalf of the institution. Such processing must be authorised by the institution, parent, guardian, law, contract or another lawful basis recognised under applicable law.

Institution and Commercial Information

The platform may process institution name, domain name, logo, contact details, subscription status, payment references, licence dates, support tickets and demo requests.

Technical Information

The platform may process IP addresses, session identifiers, browser details, device information, authentication events, security logs, error logs and audit records.

Uploaded Content and User Generated Content

Users may upload course content, PDFs, videos, SCORM packages, forum posts, comments, messages, recordings and other content. Institutions remain responsible for ensuring that uploaded content is lawful and appropriate.

How Information Is Used

Renode Technologies processes personal information to:

- Provide and operate the LMS platform.
- Authenticate users and manage sessions.
- Enforce role-based access controls.
- Deliver courses, assessments and online classes.
- Record learner progress and grades.
- Support sponsor visibility where authorised.
- Provide technical support and customer assistance.
- Process subscriptions, payments and licence status.
- Improve security, reliability and platform performance.
- Communicate service, legal and operational notices.
- Comply with legal obligations.
- Investigate misuse, fraud, security incidents or policy breaches.

Legal Basis for Processing

Depending on the context, processing may be based on:

Basis Application
--- ---
Contract Providing LMS services to institutions and users.
Consent Optional communications, cookies where required, and child-related processing where applicable.
Legal obligation Compliance with education, tax, privacy, consumer protection and cybersecurity obligations.
Legitimate interests Security monitoring, fraud prevention, support, service improvement and

operational administration.
Public interest or official authority Public-sector education programmes where applicable.
Vital interests Emergency circumstances where permitted by law.

Cookies and Tracking

The platform uses cookies and similar technologies for:

- Login sessions.
- CSRF protection.
- Security controls.
- User preferences.
- Platform performance and diagnostics.

The platform does not require advertising cookies for core LMS operation. Where analytics or tracking tools are introduced, institutions and users must be provided with appropriate notices and consent options where required by law.

Third-Party Services

The platform may integrate with:

Service Type Purpose
--- ---
PayFast Subscription and payment processing.
Jitsi Meet Online classes.
Microsoft Teams Online class joining where configured.
Google Meet Online class joining where configured.
Google Cloud Storage Storage of multimedia files and institution assets.
Google Compute Database hosting.
Google Cloud Redis Cache and performance layer.
Akamai/Linode Hosting, load balancing and content delivery.
SMTP provider Email delivery.
Google/Microsoft/OIDC SSO Institution-managed authentication.

Third-party services process information according to their own terms and privacy notices where they act as independent controllers, and according to processing agreements where they act as operators/processors.

International Data Transfers

Personal information may be processed outside South Africa where cloud, email, meeting, storage or authentication providers operate internationally. Renode Technologies and its institutional customers must ensure that cross-border transfers comply with POPIA, GDPR and applicable law. Appropriate safeguards may include contractual data processing terms, standard contractual clauses, adequacy decisions, transfer impact assessments and technical security controls.

Children’s Privacy Protections

The platform may be used by minors and school learners. Renode Technologies applies the following child protection principles:

- Processing is limited to education and platform purposes.
- Child data is institution-scoped and access-controlled.
- Sponsor or guardian visibility is explicitly mapped.

- Direct marketing to children is not part of core LMS operation.
- Communication tools are subject to institutional moderation and acceptable use controls.
- Institutions must obtain parental or guardian consent where required.
- Child data must not be retained longer than necessary.
- Security incidents involving child data must be escalated promptly.

User Rights

Depending on jurisdiction, users may have rights to:

- Access personal information.
- Correct inaccurate information.
- Request deletion where legally permitted.
- Object to processing.
- Restrict processing.
- Data portability.
- Withdraw consent where processing is based on consent.
- Opt out of certain sharing or sale of personal information where applicable.
- Not be discriminated against for exercising privacy rights.
- Lodge a complaint with a regulator.

Requests should be submitted to the relevant institution where the institution controls the record, or to Renode Technologies where Renode Technologies controls the relevant information.

Data Subject Access Requests

Renode Technologies will support data subject access requests in line with POPIA, PAIA, GDPR and applicable laws. Requests must include sufficient information to verify identity and locate the record. Where Renode Technologies acts as an operator/processor, the request may be referred to the relevant institution.

Data Retention

Personal information is retained only for as long as necessary for the purpose for which it was collected, unless a longer retention period is required by law, contract, education policy, audit obligation, dispute requirement or legitimate operational need.

Recommended retention categories include:

Data Category Retention Approach
--- ---
Active user accounts For the duration of the institution relationship or active enrolment.
Academic records According to institution policy and applicable education law.
Support tickets Retained for service history, audit and dispute management.
Payment records Retained according to tax, accounting and payment regulations.
Security logs Retained for security monitoring and incident investigation.
Demo requests Retained for commercial follow-up unless deletion is requested.

Security Measures

The platform uses administrative, technical and organisational safeguards, including:

- Password hashing with Argon2id.
- Secure session handling and inactivity timeout.
- CSRF protection.

- Role-based access control.
- Institution-level data separation.
- Controlled file access.
- Upload validation.
- Reset token expiry and hashing.
- HTTPS in production.
- Backup and disaster recovery procedures.
- Staff access controls and security awareness.

User Consent

Consent is obtained where required by law, contract or institutional policy. For child learners, consent or authorisation may need to be obtained from a competent person, parent, guardian, school authority or other authorised representative depending on the context.

Complaints Procedure

Privacy complaints may be submitted to Renode Technologies at info@renode.co.za. Complaints should include the requester's name, contact details, institution, affected account, description of the concern and requested outcome.

Where a complaint relates to an institution-controlled record, Renode Technologies may refer the matter to the relevant institution. Users may also lodge complaints with the Information Regulator of South Africa or other applicable supervisory authorities.

Cross-Border Processing Clauses

Where personal information is transferred across borders, Renode Technologies will take reasonable steps to ensure appropriate safeguards are in place, including contractual obligations, security controls, access restrictions, vendor due diligence and lawful transfer mechanisms.

CCPA/CPRA Notice

The platform is not designed to sell personal information. Where CCPA/CPRA applies, California residents may request access, deletion, correction, limitation of sensitive information use, and information about categories of personal information collected, disclosed or shared. Renode Technologies will respond according to applicable legal thresholds and verification requirements.

Updates to This Policy

Renode Technologies may update this policy to reflect legal, technical or operational changes. Material changes will be communicated through appropriate platform, contractual or website notices.

Contact Information

Renode Technologies (Pty) Ltd
Email: info@renode.co.za
Country: South Africa

References

- Protection of Personal Information Act, 2013.
- Children's Act, 2005.

- European Commission GDPR guidance.
- California CCPA/CPRA guidance.
- Information Regulator South Africa guidance.