

Vendor Privacy & Security Overview

Version 1.0 · Last Updated: June 8, 2026

About rinnalla

rinnalla is a parent-focused literacy platform designed to support families, educators, healthcare organizations, and community partners in promoting early literacy development through evidence-based coaching and learning experiences.

rinnalla's mission is to strengthen the relationship between adults and children through literacy-rich interactions while maintaining strong privacy protections and responsible data stewardship.

rinnalla is intentionally designed around a minimal-data architecture. We collect only the information necessary to provide our services, manage subscriptions, and support participating organizations.

Data Privacy Philosophy

rinnalla follows four guiding principles:

Data Minimization

We collect only the information necessary to operate the service.

Privacy by Design

Privacy considerations are incorporated into product design decisions and platform architecture.

Transparency

We clearly disclose what information is collected, how it is used, and how it is protected.

Educational Purpose

Information is used solely to provide and support educational and literacy-related services.

rinnalla does not sell personal information and does not use personal information for targeted advertising.

Information We Collect

Parent Account Information

- Parent name
- Parent email address
- Account identifier

Purpose: Account creation, authentication, customer support, and subscription management.

Child Profile Information

- Child name
- Child age

- Child grade level
- Organization affiliation (when applicable)

Examples of organization affiliation include:

- School districts
- Healthcare organizations
- Literacy organizations
- Community partners

Purpose: Personalization of learning experiences and account administration.

Account Administration Information

- Subscription status
- License status
- Transaction identifiers
- Last login timestamp

Purpose: Subscription validation, licensing administration, customer support, and service operation.

Technical Information

- Device metadata
- Application metadata
- Crash reports
- Error diagnostics
- Authentication metadata

Purpose: System reliability, troubleshooting, security, and service improvement.

Information We Do Not Collect

rinnalla does not currently collect:

- State student identification numbers
- District student identification numbers
- Social Security numbers
- Home addresses
- Phone numbers
- Race or ethnicity information
- Disability information
- IEP or 504 information
- Medical information
- Attendance records
- Discipline records
- Free or reduced lunch status
- Standardized assessment scores
- Payment card information

Educational Performance Data

At this time, detailed literacy activity data, reading performance information, and educational progress information remain local to the user's device and are not stored within **rinnalla** cloud systems.

This architecture significantly reduces privacy risk and minimizes exposure of educational performance information.

Future platform features may introduce additional educational reporting capabilities. Any material changes to data collection practices will be reflected in updated privacy documentation.

Data Storage and Hosting

Primary Infrastructure Provider: Google Firebase

Storage Region: United States

Current production cloud data is stored within the United States.

Third-Party Service Providers

rinnalla utilizes a limited number of carefully selected service providers.

Firebase

Purpose: Authentication, hosting, and cloud data storage.

RevenueCat

Purpose: Subscription management and purchase restoration.

RevenueCat does not directly process payments.

Sentry

Purpose: Crash reporting and application diagnostics.

SiteDetour

Purpose: Dynamic QR code generation, routing, and experience delivery.

Security Controls

rinnalla maintains reasonable administrative, technical, and operational safeguards designed to protect information from unauthorized access, disclosure, alteration, or destruction.

Current safeguards include:

- HTTPS encrypted communications
- Firebase authentication services
- Password hashing and secure credential management
- Role-based access controls
- Restricted administrative access
- U.S.-based cloud hosting
- Vendor security review processes
- Incident response procedures

rinnalla maintains documented Security, Data Retention, and Data Breach Response policies.

Data Deletion and Retention

rinnalla supports verified account deletion requests.

Account records may be deactivated and removed from active use while deletion is processed in accordance with the **rinnalla** Data Retention Policy.

Information is retained only as long as necessary to support legitimate business, contractual, operational, or legal requirements.

Compliance Documentation

rinnalla maintains the following governance documents:

- Data Map
- NDPA Exhibit B
- Subprocessor Registry
- Application Privacy Policy
- Information Security Policy
- Data Breach Response Plan
- Data Retention Policy

These documents are available upon request and may be provided during procurement, contracting, or privacy review processes.

Contact Information

Privacy and Compliance Inquiries:

privacy@rinnallaliteracy.com

General Support:

support@rinnallaliteracy.com

Website:

www.rinnallaliteracy.com

7984 South 1300 East, Sandy, UT 84094
801-834-1798