Student & School Data Protection Notice

Vidyaluma — A product of KRAVIA PRIVATE LIMITED

Published policy · Effective from 1 November 2026

Approved: 1 November 2026

T02 · Version 1.0.0

Child-aware safeguards, guardian relationships, school accountability and practical privacy choices.

On this page

1. What this Notice means
2. Plain-language student and parent explanation
3. Necessary information and restrictions
4. Consent and guardian authority
5. Guardianship changes and multiple institutions
6. Academic records, AI and appeals
7. Communication, safeguarding and location
8. Adult verification does not become student KYC
9. Privacy requests, retention and security
10. Complaints and review

▶ On this page

1. What this Notice means

1.a — Vidyaluma and the school. Vidyaluma is software provided by KRAVIA PRIVATE LIMITED to authorized schools and institutions. Schools use enabled functions to manage their work and provide school-controlled access. The school normally decides the educational purpose of its records; KRAVIA must protect and process them appropriately and remains responsible for its own activities and defects.

1.b — Audience. This Notice is for students, parents, guardians, teachers and school administrators. A school purchasing a subscription does not mean every user is an adult. Public material must not claim that Vidyaluma is adult-only while the app is actually used by children.

2. Plain-language student and parent explanation

Skip to content

2.a — What happens. Your school may use Vidyaluma for information such as your class, attendance, schoolwork, marks, approved reports and messages. Only the people with a relevant authorized role should see protected information. Another school must not be able to look at it just because it uses Vidyaluma too.

2.b — Choices and help. Ask your school about a mark or attendance correction. You or your guardian can also contact Vidyaluma about privacy, unsafe content or a technical problem. Use /privacy-request or support@vidyaluma.in. Do not send a password, OTP, Aadhaar number or another student's records in an ordinary message.

2.c — AI. Some enabled tools may help a teacher prepare feedback or other schoolwork. AI can make mistakes. A responsible teacher must review important results; AI is not allowed to decide your punishment, admission or medical condition. You can report a result or answer that seems wrong or harmful.

3. Necessary information and restrictions

3.a — Limited collection. Each enabled school activity must specify what information is needed and why. Optional information is identified as optional. Fields for health, disability, welfare, discipline or identity material must not be added simply because they might be useful later.

3.b — No unrelated exploitation. Student information must not be sold, used for targeted advertising, used for unrelated commercial profiling or used to train general-purpose AI models. Private school content must not be shared across KRAVIA products for undisclosed purposes. Codes or removed names do not automatically make a student record anonymous.

3.c — Images and biometrics. Authorized school photographs may support a legitimate school activity, with appropriate permission and restricted visibility. Public promotion requires separate authorization. Student biometric attendance, AI face identification, emotion inference and attention/behavior scoring from images are not permitted default uses.

4. Consent and guardian authority

4.a — Appropriate authority. Schools and KRAVIA must identify the notices, legal basis and verified parent/guardian consent required for the actual activity. Institutional authorization is not a blanket substitute. Any relied-on education exemption needs a scoped legal assessment; it must not be assumed to cover a commercial vendor's separate analytics or marketing.

4.b — Usable choices. Optional AI, marketing or tracking choices are separate from essential educational access. A child or family must not be pressured to supply unnecessary data by a threat to marks or basic school participation. When a required lawful permission is absent, the affected processing is restricted and an appropriate alternative is considered.

4.c — Withdrawal. Withdrawal stops the processing that depends on that permission, subject to a separate lawful and clearly explained retention requirement. It does not automatically erase an already valid academic record or signed adult agreement. We distinguish the specific purpose and data rather than claiming that all information may be kept indefinitely.

5. Guardianship changes and multiple institutions

5.a — Conflicts. Separated parents, disputed guardians, restricted-access orders and school-transfer situations require careful authority review. A shared surname or phone number does not prove the right to obtain records. Disclosures are limited while contradictory claims are evaluated.

Skip to content

5.b — Becoming an adult. When a student reaches adulthood, account and guardian-access arrangements require review according to applicable rights and school rules. Previous parental involvement must not automatically create permanent access to the adult student's private information.

5.c — Transfers. A move between schools does not authorize both schools to browse each other's records. Authorized export or transfer must identify the recipient, purpose and relevant records and preserve restrictions and source history. A school closure or ownership change requires verified legal authority before protected information is handed over.

6. Academic records, AI and appeals

6.a — Accuracy. Schools verify educational inputs and approve changes to attendance, grades and official reports. KRAVIA supplies secure correction and audit mechanisms and investigates software-caused mistakes. Necessary original evidence is preserved so a changed result can be understood.

6.b — AI restrictions. AI-generated marks and important educational reports remain drafts until qualified school personnel approve them. Predictions are advisory, not guaranteed results or diagnoses. AI must not independently determine admission, discipline, guilt, expulsion or staff employment outcomes.

6.c — Appeals. A student or guardian can request academic review from the school and report suspected system or AI faults to KRAVIA. A report should receive a meaningful route and avoid retaliation. When an erroneous result was already published, authorized correction and appropriate recipient notification must be considered.

7. Communication, safeguarding and location

7.a — Safe communications. Educational messages require appropriate roles, verified recipients and child-safety controls. Bullying, harassment, threats, exploitation and unauthorized adult-child contact can be reported. Access to reports is restricted to appropriate reviewers and safeguarding personnel rather than made public.

7.b — Monitoring boundaries. Safeguarding is not permission for unlimited private-message surveillance or indiscriminate employee access. The purpose, authorized viewers and retention must be defined. Immediate danger should also be raised directly through appropriate emergency and school channels; the app is not a substitute for them.

7.c — Transport. Approved vehicle tracking is limited to authorized adult driver/staff devices and relevant trips. Parent visibility must be scoped to the appropriate route and child association. Continuous child-device location or child behavioral profiling cannot be introduced under a general transport clause.

8. Adult verification does not become student KYC

8.a — Separate onboarding. OVSE/Aadhaar App and DigiLocker in the recorded Vidyaluma scope concern adult school representatives. They are not student attendance or KYC mechanisms. A student or parent must not be asked for Aadhaar simply because the school representative used it during contracting.

8.b — Signing. Leegality executes an authorized adult school's agreement through a separate informed process. A parent's ordinary app access is not acceptance of an institutional signing obligation. Provider identity verification does not establish school authority or government endorsement.

9. Privacy requests, retention and security

9.a — Requests. Students, guardians and other individuals can initiate appropriate access, correction, export or deletion requests without being the paying school. School-record decisions and KRAVIA's independent

Skip to content

responsibilities are distinguished. Necessary identity verification is proportionate and uses a protected channel.

9.b — Deletion. Account deletion is not merely deactivation. Any retained educational, agreement, security or financial record needs a specific lawful purpose and access restriction. T07 controls school exit, backups and provider deletion. Subscription disputes must not automatically prevent an individual's valid request.

9.c — Incidents. KRAVIA and schools coordinate notifications according to their actual legal responsibilities. KRAVIA must address its own incident duties and assist the school; it cannot assign every notification to the school by policy wording alone. Student information must not be exposed in a public incident summary.

10. Complaints and review

10.a — Assistance. Privacy, accessibility, safety and inaccurate-data complaints may be raised through support@vidyaluma.in and the applicable public request/report routes. The process in L10 provides escalation and preserves external rights. No universal waiver is imposed on a child or guardian.

10.b — Governance. This Notice is original Vidyaluma content maintained through approved source releases. Changes to child-facing features, provider data use, audience age or consent practices require review before activation. Appropriate understandable language and accessible alternatives are part of that review, not optional decorative additions.

Related documents
L01 — Privacy PolicyL04 — Acceptable Use PolicyL06 — Accessibility StatementL09 — Data Processing AgreementL10 — Grievance, Complaints & Appeals PolicyT03 — Responsible AI PolicyT05 — School Control, Access & Sharing StatementT07 — Data Retention, Export & Deletion Policy

The current published version is shown. Earlier review copies do not create customer acceptance or contractual terms.

Vidyaluma

VidyaLuma

Clear school work, calmer daily decisions, and trusted records in one connected place.

Book a walkthrough

Contact support

Explore

About

Product

School support

Book a walkthrough

Contact

Trust

Security & Service Reliability Statement

Legal

Privacy Policy

Terms & Conditions

Skip to content

Pricing

Guides

Release notes

FAQs

Verify partner ID

Status

Student & School Data Protection Notice

Responsible AI Policy

Data Use & Purpose Limitation Statement

School Control, Access & Sharing Statement

Subprocessor & International Processing Notice

Data Retention, Export & Deletion Policy

Vulnerability Disclosure Policy

Cookie & Tracking Technologies Policy

Acceptable Use Policy

Disclaimer

Accessibility Statement

Billing, Subscription, Cancellation & Refund Policy

Support & Service Commitments Policy

Data Processing Agreement

Grievance, Complaints & Appeals Policy

School-controlled sharing **Role-aware access** **GST included in public pricing**

Built for school teams that need clear, trusted operations. Made in India, with love ❤ Copyright 2026 Vidyaluma. All rights reserved.

Legal Trust Privacy request Delete an account Service status Cookie choices Back to top ↑