Data Use & Purpose Limitation Statement

Vidyaluma — A product of KRAVIA PRIVATE LIMITED

Published policy · Effective from 1 November 2026

Approved: 1 November 2026

T04 · Version 1.0.0

What school information may be used for, what is prohibited, and how new purposes are controlled.

On this page

1. Purpose and responsible parties
2. School-workflow purposes
3. Service operations and support
4. Uses that are not authorized
5. AI processing and provider use
6. Identity, document and agreement purposes
7. Sharing, aggregation and business transfers
8. Retention, rights and purpose changes

▶ On this page

1. Purpose and responsible parties

1.a — Scope. Vidyaluma, a product of KRAVIA PRIVATE LIMITED, processes information only for an identified authorized purpose. This Statement covers school workflows, service operations, AI tasks, support and limited permitted measurement. It complements L01 and L09 and does not create a new blanket permission to process everything a school holds.

1.b — Role distinction. Schools generally direct the educational use of their records. KRAVIA has separate responsibilities for its own contracting, subscription administration, security, public enquiries and other independent activities. Actual purposes and control determine responsibility; a written label cannot reassign statutory duties.

2. School-workflow purposes

2.a — Enabled functions. Relevant data may be used to administer authorized accounts, attendance, assessments, reports, communications, fee records, documents and other specifically enabled school functions. Only the fields needed for the actual function are permitted. Mentioning a module does not verify its production availability or authorize its collection in every app.

2.b — User context. Information use is bounded by school membership, role, current permission and the requested task. A teacher preparing one class's report does not automatically need the full institution's welfare or payment records. A student's membership in two schools does not create a shared private profile between them.

2.c — Source quality. Records must identify relevant source, person and school association. Incorrect marks, attendance or guardian data follow a controlled correction route. KRAVIA investigates processing defects and the school verifies educational decisions, preserving meaningful audit history.

3. Service operations and support

3.a — Necessary operation. KRAVIA may process limited information to authenticate users, secure services, reconcile subscriptions, respond to requests, diagnose failures and maintain justified legal evidence. Each activity requires a defined purpose and appropriate limits; a general desire to improve the product is not permission for unrestricted access to school content.

3.b — Support access. Authorized staff use only information necessary for the reported issue, with proportionate verification and auditable access. A support ticket must not expose unrelated students, grant permanent impersonation privileges or be copied wholesale to an unapproved external AI service.

3.c — Testing and improvement. Prefer synthetic, public-domain, appropriately licensed or genuinely anonymized non-identifiable test data. Private school material is not a default development dataset. Access to exceptional evidence requires a specific justification and safeguards, and must not contradict the no-training rule in T03.

4. Uses that are not authorized

4.a — Sale and marketing. Student information must not be sold, traded, used for targeted advertising or repurposed for unrelated commercial profiling. School-provided access is not consent to marketing from every KRAVIA product. Public use of school logos or student images requires separate appropriate permission.

4.b — Sensitive inference. Vidyaluma must not use school images or records for AI facial recognition, emotion/attention scoring, psychological diagnosis or hidden behavioral classifications. Restricted health, disability, disciplinary and government-identity information remains excluded from ordinary AI features by default.

4.c — Unauthorized decisions. Data must not be used by AI to autonomously determine identity, contracting authority, signatures, final exam marks, admissions, discipline or employment. A school's access setting cannot authorize a legally prohibited use or remove necessary human accountability.

5. AI processing and provider use

5.a — Minimum context. An approved AI task may receive only the necessary permitted context. Private school records, prompts, outputs and conversations must not train or fine-tune general-purpose models for KRAVIA or its providers. Removing a name does not create automatic authorization for reuse.

5.b — Provider retention. Model inference, abuse review, logs and training are distinct activities. The exact provider tier and terms must support the permitted use and be disclosed appropriately. No training claim is made about an unreviewed provider, and a new fallback is not automatically approved.

Skip to content

5.c — Retrieval and revocation. Retrieval must enforce school and source permissions, including deletion and revocation. Relevant indexes, embeddings and caches must not preserve a hidden access route after the source or user authorization ends.

6. Identity, document and agreement purposes

6.a — OVSE. Approved Aadhaar offline verification concerns an adult school representative's identity for onboarding. It is not a student KYC, attendance, advertising or AI-input source. Required purpose-specific consent, alternatives, minimal data and stricter provider conditions apply.

6.b — DigiLocker. Retrieval is limited to selected permitted documents necessary for authorized adult onboarding. Unrestricted browsing, routine teacher login and automatic school-authority decisions are outside the defined scope. The representative's provider credentials must not be collected by Vidyaluma.

6.c — Leegality. Relevant signatory data and agreement content are used for the configured execution workflow and justified evidence. Optional photo, liveness, GPS or notification functions require review and disclosure when actually enabled. Verification permission is not agreement signing consent.

7. Sharing, aggregation and business transfers

7.a — Recipients. School-directed sharing identifies an authorized recipient and limited record scope. Providers receive only data needed for reviewed services. A verified provider schedule must identify actual recipients and roles; an unspecified "trusted partners" category is not enough to justify new disclosure.

7.b — Aggregates. Statistical outputs must not reasonably identify a person, small group or confidential school fact. Anonymization requires a defensible assessment of re-identification and linkage risks. Pseudonymous identifiers, small cohorts and private free text are not automatically anonymous.

7.c — Business events. A merger or service transfer requires a lawful purpose, restricted diligence, confidentiality and required notices. It is not a route to sell student profiles or erase existing purpose limits. Mandatory rights and applicable contracts continue to govern.

8. Retention, rights and purpose changes

8.a — Retention. Data must not outlive its justified purpose merely because storage is inexpensive. Category-specific schedules, limited legal holds, provider cleanup and backup rotation are governed by T07. Continued security or legal retention does not authorize renewed use for teaching, marketing or AI.

8.b — Requests. People can raise access, correction, export, deletion or consent-withdrawal requests at /privacy-request or support@vidyaluma.in. School-controlled educational decisions and KRAVIA's independent processing are assessed separately. A privacy complaint is not automatically closed by referring the person to their school.

8.c — New purpose approval. A materially different use requires a fresh assessment of necessity, law, permissions, notice, provider terms and safeguards before activation. Appropriate additional consent or contractual change must precede processing. The policy itself changes only through reviewed source releases, not an admin setting or AI instruction.

Related documents
L01 — Privacy PolicyL03 — Cookie & Tracking Technologies PolicyL09 — Data Processing AgreementT02 — Student & School Data Protection NoticeT03 — Responsible AI PolicyT05 — School Control, Access & Sharing StatementT06 — Subprocessor & International Processing NoticeT07 — Data Retention, Export & Deletion Policy

Skip to content

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

VidyaLuma

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

Book a walkthrough **Contact support**

Explore

About
Product
Pricing
Guides
Release notes
FAQs

School support

Book a walkthrough
Contact
Verify partner ID
Status

Trust

Security & Service Reliability Statement
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

Legal

Privacy Policy
Terms & Conditions
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 ↑