Privacy Policy

Vidyaluma — A product of KRAVIA PRIVATE LIMITED

Published policy · Effective from 1 November 2026

Approved: 1 November 2026

L01 · Version 1.0.0

How Vidyaluma handles personal information across its public website, school services, mobile experiences and adult-representative onboarding.

On this page

1. Identity, scope and application
2. The school and KRAVIA have different responsibilities
3. Information used in the service
4. Sources, purposes and necessary collection
5. Children, guardians and school authorization
6. AI-assisted processing
7. Device permissions and transport information
8. OVSE, DigiLocker and Leegality
9. Recipients and onward disclosure
10. Storage locations and security
11. Retention and deletion
12. Access, correction, export and account deletion
13. Marketing, publication and policy changes

▶ On this page

1. Identity, scope and application

1.a — Operator. Vidyaluma is a product of KRAVIA PRIVATE LIMITED ("KRAVIA", "we", "us"). This Policy explains the handling of personal information connected with Vidyaluma. It covers public enquiries, school-managed accounts, enabled educational and administrative services, authorized support, subscription administration and adult school-representative verification. It does not make every KRAVIA product subject to identical processing practices.

Skip to content

1.b — Initial market. Vidyaluma's initial commercial offering is for schools and institutions in India. An authorized adult contracts for the school; a student is not made the purchaser by using school-provided access. A visitor outside India may read public material, but access alone does not establish an international service offering or remove rights that otherwise apply.

1.c — Dates. The effective date for this policy set is 1 November 2026. Publication does not create retrospective notice, consent, acceptance or legal compliance. The actual publication record and the version applicable to a particular transaction must remain identifiable.

2. The school and KRAVIA have different responsibilities

2.a — School instructions. Schools normally determine the educational purposes for which their student, guardian and staff records are handled, identify authorized users and decide academic corrections and disclosures. KRAVIA handles those records to provide the instructed service, subject to the applicable Data Processing Agreement (L09) and its independent obligations. A contractual label cannot override the actual purpose and control of processing.

2.b — KRAVIA's own activities. KRAVIA separately determines necessary purposes for operating its public website, responding to enquiries, establishing customer authority, managing its contracts and subscriptions, protecting the service and meeting its own legal obligations. These activities must not become an undisclosed route to reuse educational records for advertising, unrelated products or AI training.

2.c — Individual rights. A school's administrative control does not mean that it owns a person's privacy rights. We assess requests according to the relevant records, lawful authority and applicable obligations. We do not automatically refuse a privacy complaint because the complainant is not the paying school.

3. Information used in the service

3.a — Website and customer contact. Enquiries may include the sender's name, school or organization, role, contact details, stated requirements and message. Subscription and onboarding records may include authorized-representative details, authority evidence, selected plan, invoicing information and transaction references. Public forms must not request student records, passwords, OTPs or full government-identity documents.

3.b — School records. Enabled school workflows may require student and staff identifiers, class and role assignments, guardian associations, attendance, assessments, answer-sheet images, marks, feedback, approved reports, school communications and document records. Fee-ledger entries are distinct from payment authentication details. A module's inclusion here describes its permitted processing boundary, not proof that it is available in every school or app version.

3.c — Restricted information. Health, disability, disciplinary, welfare or government-identity information is not a default input to ordinary AI or public contact features. A school must identify a necessary permitted purpose and appropriate authority before any restricted workflow is enabled. Biometric attendance, facial recognition and emotion inference are not default Vidyaluma services.

3.d — Technical information. Necessary service operation may involve account and session references, IP addresses, access events, device or browser attributes, crash diagnostics, notification tokens and security logs. Optional visitor analytics have a separate consent gate. We must not convert technical logs into unrestricted archives of messages, answer sheets, identity documents or secret credentials.

3.e — Specialist registration methods. A Vidyaluma specialist account may be created or invited by an authorised school or operations administrator through the existing access-provisioning workflow, or submitted independently through Vidyaluma Launchpad. An administrator-provided invitation is not consent to identity-

document processing. The specialist receives the applicable notice, can request correction of account information and must provide their own explicit consent before identity evidence is uploaded.

3.f — Specialist application information. The Launchpad self-registration form currently asks for a specialist's name, email address, mobile number, city, state, school coverage area, relevant experience, password and application-consent record. The identity step asks the specialist to choose Aadhaar or another government-issued identity-document route, provide the last four Aadhaar digits only when Aadhaar is selected, and provide front/back document images, a selfie, a camera-captured live picture and image-quality confirmations. The current implementation records evidence for manual review; it does not claim facial recognition, biometric matching, automated liveness or UIDAI authentication.

4. Sources, purposes and necessary collection

4.a — Sources. Information can come from an individual, their authorized school, an approved import, an authorized guardian or a provider involved in the specific transaction. We must preserve the source and school association needed to check a record. Publicly accessible information is not automatically available for unlimited collection or reuse.

4.b — Permitted purposes. We use relevant information to provide school workflows, authenticate and authorize access, process instructed records, respond to support and rights requests, maintain security, reconcile subscriptions and preserve justified evidence. Each category must have an identifiable purpose, access owner and retention rule. We do not collect information merely because a provider API exposes it.

4.c — Choices and consequences. Required and optional fields must be distinguishable. Refusing optional analytics, marketing or an optional AI feature must not silently remove unrelated core access. A necessary verification step may remain incomplete until an approved alternative succeeds; this must be explained without treating refusal of optional Aadhaar use as proof of wrongdoing.

5. Children, guardians and school authorization

5.a — Child-aware service. Students may be children even though the school's purchaser is an adult. We require age-appropriate access and notices, verified school associations, restricted sharing and appropriate parent or guardian authorization where required. School permission alone is not treated as a universal substitute for legally required parental consent.

5.b — Protected uses. Student information must not be sold, used for targeted advertising or used for unrelated commercial profiling. We prohibit AI emotion detection, facial identification and autonomous decisions on discipline, admissions or employment. Learning assistance must not become a hidden personal-risk classification or diagnosis.

5.c — Conflicting requests. Questions about guardianship, restricted parent access, a student reaching adulthood or conflicting school instructions are reviewed before protected records are disclosed or changed. We request proportionate evidence through a secure channel and explain any restriction. The Student and School Data Protection Notice (T02) supplies the fuller child-facing safeguards.

6. AI-assisted processing

6.a — Task-limited assistance. Where enabled, AI may assist with extraction, summaries, feedback, draft educational materials or analysis relevant to an authorized school task. Only necessary task content and permitted context may be sent to an approved AI service. Important outputs must distinguish generated drafts from school-approved records and identify relevant uncertainty.

Skip to content

6.b — No model training on school content. KRAVIA must not use private student, teacher, guardian or school content to train or fine-tune general-purpose models, and must not authorize its AI providers to do so. Replacing names with codes does not remove that restriction. Necessary execution of a school's requested AI task is distinct from model training. Provider terms, service tier, logging and abuse-review behavior must support this commitment before use.

6.c — Review and errors. AI does not decide final examination marks, admissions, discipline, employment, identity verification or school authority. Authorized people review consequential outcomes. Users can report harmful or inaccurate output, and KRAVIA investigates attributable system defects while the school manages academic reassessment. T03 governs these uses and limitations.

7. Device permissions and transport information

7.a — Purpose-specific permissions. Camera and selected-file access may support approved scanning or uploads; notifications may deliver authorized service messages. Microphone or location access requires a specific enabled function and a clear explanation. The mobile operating-system permission is not a substitute for an appropriate privacy disclosure or other necessary authorization.

7.b — Location boundary. Approved transport tracking must be limited to authorized adult driver or staff devices and relevant trip periods, with scoped recipient access. We do not make continuous child-device tracking a condition of ordinary school access. Any proposed child-location feature requires a separate legal and distribution-policy assessment before enablement.

7.c — Local copies. School data cached on a shared or offline device must have a defined protection and cleanup process. Logout, membership removal and lost-device response must address sessions and cached access. Users should avoid retaining school downloads on shared devices after their authorized need ends.

8. OVSE, DigiLocker and Leegality

8.a — OVSE identity verification. Aadhaar offline verification, where enabled under the approved OVSE arrangement, is limited to authorized adult school representatives. The representative must receive a purpose-specific disclosure, choose what permitted information is shared and have an appropriate viable alternative. Identity verification is not school-authority verification, government endorsement or agreement execution.

8.b — DigiLocker document retrieval. The representative authenticates with the provider and authorizes access to selected, permitted documents needed for onboarding. Vidyaluma must not collect their DigiLocker password or OTP, browse unrelated documents, use this flow for student KYC or automatically activate the school. Retrieved document integrity and representative authority are reviewed separately.

8.c — Leegality signing. Agreement execution is a separate signing transaction. Relevant representative details, agreement contents and signing evidence may be handled by Leegality and the selected signing service. We must disclose the actual configured method and any extra photo, liveness or location collection before it occurs. A provider offering a feature does not mean Vidyaluma has enabled it.

8.d — Evidence and withdrawal. Only necessary, permitted verification outcomes and references may be retained. Temporary tokens, raw identity payloads and unnecessary copies must be removed according to the approved transaction rules. A withdrawal stops further consent-dependent processing; any retained evidence needs a specific lawful reason and must respect stricter OVSE or provider deletion conditions. Lawfully executed agreements require a separate retention assessment.

8.e — Specialist identity verification. Launchpad may request identity documentation and a verification photograph during specialist onboarding to help confirm identity, reduce impersonation and fraudulent registrations and support a trusted school environment. Aadhaar, where supported, is voluntary and is not proof

of Indian citizenship or domicile. The current Launchpad flow stores only the last four Aadhaar digits in application state, requires the specialist to confirm that the first eight digits are hidden in both uploaded Aadhaar images and routes the masked evidence to authorised manual review. The application does not perform automated image redaction, UIDAI authentication, facial recognition, biometric matching or an automated liveness decision; the masking confirmation remains subject to manual review. A specialist may choose the implemented manual route for another government-issued identity document; the document type and lawful review basis must be confirmed before public activation.

8.f — Identity-verification consent. Before any identity upload, Launchpad presents a standalone notice that identifies the evidence requested, the purpose, the access boundary, the retention approach and the rights route. An unchecked, purpose-specific consent is recorded with the notice version, purpose and acceptance time. Consent is enforced by the server; an administrator-created account or invitation does not substitute for the specialist's consent.

9. Recipients and onward disclosure

9.a — Service recipients. Appropriate data may be handled by reviewed infrastructure, communications, payment, security, verification, signing and AI providers for the specified service. Access is limited by purpose and contract. The Subprocessor and International Processing Notice (T06) and its verified provider schedule must identify active recipients; a broad category is not a substitute for that schedule.

9.b — School-directed sharing. Authorized school users may share selected reports with verified guardians or other permitted recipients. Scope, expiry and revocation apply where the product supports them. A downloaded copy or external recipient may remain outside technical revocation; the school must still respect the person's rights and onward-sharing limits.

9.c — Legal and business events. KRAVIA verifies competent legal requests, limits disclosure to what is required, preserves relevant evidence and provides notice where permitted. A merger or business transfer requires privacy review, suitable safeguards and required notifications. It does not authorize a sale of student data for unrelated marketing.

9.d — Specialist access boundary. School administrators may receive only the application and verification status needed to manage their specialists. Raw identity documents and verification photographs remain restricted to specifically authorised Vidyaluma reviewers and necessary contracted infrastructure providers subject to confidentiality and security obligations. A school administrator must not receive unrestricted access to the underlying identity documents.

10. Storage locations and security

10.a — India-first, not an absolute localization assertion. Indian regions are the preferred storage direction for school records. Remote support, provider processing, logs and backups can affect the actual location. We must disclose and assess any necessary international processing before activation and comply with applicable restrictions; this Policy does not certify that every byte remains in India.

10.b — Required safeguards. Access limitation, encryption, tenant separation, privileged-account protection, audit records, vulnerability management and recovery controls must be appropriate to the data and supported by evidence. Authorized staff access is purpose-limited and reviewed. We do not claim perfect security, zero data loss or a certification that has not been obtained for Vidyaluma.

10.c — Incident response. We investigate suspected incidents, contain harm, preserve necessary evidence, coordinate with affected schools and meet applicable notification duties. We do not wait for a final forensic report to start a legally required notification. Public updates must not expose student details or information that would worsen the incident.

10.d — Specialist uploads, logs and delivery. Launchpad identity uploads use short-lived token-bound intents, size and content-type validation, checksums and private object keys. Raw identity images, full Aadhaar numbers, upload tokens and unnecessary personal data must not enter ordinary logs, analytics, error reports, emails or public URLs. The application response exposes review status rather than storage keys or raw document content. Exact storage encryption, provider processing and backup controls remain subject to verified runtime and subprocessor evidence.

11. Retention and deletion

11.a — Purpose and triggers. Information is retained for the necessary instructed service, justified contract administration, security, complaints and applicable legal obligations. T07 distinguishes school records, temporary verification data, AI processing material, signed agreements, financial records and restricted logs. A lawful hold must be scoped, authorized and reviewed, not applied permanently to an entire school database.

11.b — School exit. The recorded standard exit direction is a 30-calendar-day authorized export opportunity following termination, subject to any required extension or different enforceable agreement. Deletion follows the approved category-specific schedule after notice. The export window is not a universal deletion period for every record or an excuse to refuse an individual's valid request during an active subscription.

11.c — Optional measurement. The proposed maximums are 30 days for permitted public-site session recordings and 14 months for identifiable visitor analytics, with shorter retention where appropriate. These are retention ceilings, not authorization to activate trackers. Withdrawal stops new optional tracking; identifiable retained records are assessed for deletion separately.

11.d — Replicas and backups. Deletion must propagate to relevant active stores, indexes, caches, AI retrieval material and providers. Restricted backups follow the verified rotation schedule, cannot become an alternate active database and must reapply deletion instructions on restoration. We explain justified exceptions and unresolved provider cleanup rather than issuing a false completion notice.

11.e — Specialist verification retention. Identity materials are retained only for the approved identity-review, security, dispute and legal purposes and deleted through the verified category-specific process when no longer needed. The current source does not establish a standalone duration or completed raw-file deletion workflow for Launchpad identity uploads; this Policy therefore makes no shorter deletion promise. The retention schedule and backup-deletion procedure must be verified before publication.

12. Access, correction, export and account deletion

12.a — Request routes. Use Vidyaluma's Privacy Request page at /privacy-request or contact support@vidyaluma.in with the subject "Privacy request". A person without a school work email or current paid account may still raise a concern. Provide a description and relevant non-sensitive reference; do not send passwords, OTPs or full identity documents in ordinary email.

12.b — Account deletion. Users must be able to initiate deletion in the app and through the public web request route without reinstalling the app. We verify relevant identity and authority proportionately, remove eligible account data and explain any specific school-record or legal retention exception. Freezing the account, unlinking a login or withdrawing access alone is not represented as deletion.

12.c — School records. For an instructed educational record, we coordinate with the school and identify who can authorize a correction or disclosure. We still address KRAVIA's own processing and failures. Requests must not be automatically blocked because the school has an unpaid subscription, has closed, or has not supplied a usable support contact.

Skip to content

12.d — Response and appeal. We track requests, apply applicable response deadlines, communicate necessary clarification or justified delay and explain the outcome. A refusal identifies the reason to the extent permitted and an escalation path under L10. This process does not remove a right to approach an appropriate authority or competent forum.

12.e — Specialist rights and withdrawal. A specialist may use /privacy-request or support@vidyaluma.in to request access, correction, erasure where legally applicable or withdrawal of applicable identity-verification consent. Withdrawal may stop identity-dependent review or verified specialist status; it does not automatically erase records subject to a lawful hold, an executed agreement or another verified legal requirement. Specialists must not send full Aadhaar images, OTPs or passwords by ordinary email.

13. Marketing, publication and policy changes

13.a — Communications. Necessary service and school communications are separate from optional promotions. Marketing must have appropriate authorization, identify its sender and provide an effective opt-out. Joining Vidyaluma does not subscribe a person to every KRAVIA product. Public use of student images, school logos or testimonials requires separate appropriate permission.

13.b — Policy integrity. Policies are read-only through websites, apps, portals and application APIs. Approved source-code releases preserve version history and exact acceptance evidence. Merely reading this notice is not consent to optional processing or agreement to every linked document.

13.c — Changes and contact. Material changes receive appropriate notice and renewed consent or agreement where required. The actual published version and its dates must be available. Contact KRAVIA through support@vidyaluma.in or the formal channels specified in L10; required named-officer and corporate disclosures must be completed before release. No clause waives mandatory privacy rights.

13.d — Launchpad notice and review status. The specialist registration notice links directly to this Privacy Policy before identity evidence is collected and explains that administrator-created and self-registered accounts follow the same consent boundary. This policy is published for public reference. Its commitments do not imply an unverified retention schedule, active subprocessor, identity provider or identity-evidence workflow.

Related documents
L02 — Terms & ConditionsL03 — Cookie & Tracking Technologies PolicyL09 — Data Processing AgreementL10 — Grievance, Complaints & Appeals PolicyT02 — Student & School Data Protection NoticeT03 — Responsible AI PolicyT06 — Subprocessor & International Processing NoticeT07 — Data Retention, Export & Deletion Policy

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

Vidyaluma
VidyaLuma
Skip to content

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 ↑