Data Processing Agreement

Vidyaluma — A product of KRAVIA PRIVATE LIMITED

Published policy · Effective from 1 November 2026

Approved: 1 November 2026

L09 · Version 1.0.0

Standard institutional processing terms, instructions, safeguards, assistance, providers and exit responsibilities.

On this page

1. Parties, incorporation and scope
2. Subject matter, duration and processing description
3. Documented instructions and purpose limits
4. School obligations
5. Confidentiality and personnel
6. Technical and organizational safeguards
7. Subprocessors and other recipients
8. International processing
9. AI and high-risk decisions
10. OVSE, DigiLocker and Leegality boundaries
11. Rights requests and assistance
12. Personal-data incidents
13. Audits, assurance and lawful requests
14. Return, deletion and end of processing
15. Contractual remedies and duration
16. Appendix A — Required assurance schedule

▶ On this page

1. Parties, incorporation and scope

1.a — Parties. This Data Processing Agreement ("DPA") is the standard processing framework between KRAVIA PRIVATE LIMITED, provider of Vidyaluma, and the school or institution identified in an executed service agreement or order that incorporates this DPA. The customer-specific agreement identifies the contracting entity and authorized signatories. This public draft is not an executed agreement with an unnamed school.

1.b — Covered processing. The DPA covers personal information entrusted to KRAVIA to perform the school's documented educational and administrative instructions. It does not automatically classify KRAVIA's separate public-enquiry, contracting, billing, security or legal-obligation activities as processing solely for the school; L01 describes those activities. Roles depend on actual purposes and control and applicable law.

1.c — Priority. Mandatory law prevails. For instructed personal-data processing, this DPA prevails over inconsistent general service wording unless a valid specifically negotiated term provides an applicable different arrangement without reducing mandatory protection. Public Trust pages explain controls but cannot silently amend this agreement.

2. Subject matter, duration and processing description

2.a — Subject matter. KRAVIA supplies the enabled Vidyaluma school workflows identified by the accepted order, such as account administration, attendance, assessment processing, reports, communications, fee records and documents. An unpurchased or unverified module is not activated by its mention in this DPA.

2.b — Nature of operations. Authorized operations can include collection from approved sources, storage, organization, validation, retrieval, display, transmission to permitted recipients, controlled AI assistance, correction, export, restriction and deletion. Each operation must remain within the documented purpose, school context, access rules and retention schedule.

2.c — Duration. Processing lasts for the contracted service and authorized exit handling, except for a scoped legally required preservation period. The 1 November 2026 effective date does not create an earlier contract or authorize processing before proper instructions and any required notice or consent.

2.d — People and data. Covered people include students, parents/guardians, teachers, staff and authorized representatives. Covered data is limited to the categories needed for enabled modules: relevant identifiers and contacts, school/role relationships, educational records, communications, documents and transaction metadata. Restricted health, welfare, disciplinary or identity data requires a specifically approved purpose and controls; it is not authorized for general AI ingestion.

3. Documented instructions and purpose limits

3.a — Instructions. Instructions arise from the executed service documents, authorized configuration and properly authenticated requests within the agreed service. KRAVIA verifies authority for consequential actions. A password, spreadsheet upload or API call is not sufficient where the proposed action requires a higher level of authorization.

3.b — Unlawful or conflicting requests. KRAVIA informs the school when an instruction appears to exceed authority, conflict with applicable requirements or risk another person's rights, and may pause the affected operation for review. The pause must be proportionate. A manual reviewer cannot override withdrawn consent, invalid document integrity or a missing provider permission.

3.c — No unrelated reuse. KRAVIA must not sell entrusted personal information, use it for unrelated advertising, combine schools' private data for unauthorized purposes or use school content for general-purpose AI training/fine-tuning. Pseudonymizing a record does not automatically remove these restrictions. Any genuinely separate lawful purpose needs its own assessment, transparency and authorization.

4. School obligations

4.a — Lawful source and authority. The school establishes its authority to supply records and issue instructions, provides appropriate notices and required permissions, identifies correct guardian relationships and

supplies accurate relevant data. It keeps its authorized contacts and permissions current and does not instruct prohibited processing.

4.b — Children and decisions. Where required, the school obtains and can demonstrate appropriate parent/guardian authorization; it may not assume that institutional purchase replaces every child-data requirement. The school retains responsibility for qualified academic, safeguarding, discipline, admissions and employment decisions.

4.c — Cooperation. The school reasonably assists with rights requests, incidents, corrections and secure exit. A duty to cooperate does not make it responsible for defects, security failures or unlawful independent processing attributable to KRAVIA. Multi-school users and disputed authority require particular care before disclosure or transfer.

5. Confidentiality and personnel

5.a — Access need. KRAVIA restricts access to authorized personnel and providers who need it for the agreed purpose and are bound by appropriate confidentiality obligations. Roles, privileged access, support access and departures require managed approval, review and revocation.

5.b — Misuse. Unauthorized employee access, copying or disclosure is contained and investigated. Necessary evidence is preserved, affected access suspended where appropriate and applicable notification obligations fulfilled. Disciplinary or contractual action is proportionate and does not substitute for remediating the underlying access-control defect.

5.c — Continued duty. Confidentiality and lawful retention restrictions survive the end of employment, provider access or service. Confidential material must not be used in an unrelated product, demonstration, training dataset or public support conversation.

6. Technical and organizational safeguards

6.a — Baseline. KRAVIA maintains safeguards appropriate to the sensitivity and risk, including tenant separation, authorization, secure authentication, encryption appropriate to transmission and storage, privileged-account protection, audit controls, vulnerability management and recovery planning. Appendix A identifies the required assurance areas; evidence of actual deployment must support the specific commitments made to the school.

6.b — Testing and change. Material processing changes receive security/privacy review and relevant regression tests. Cross-school access, source revocation, deleted-record restoration and provider callback failures must be considered. Tests must not use unnecessary real child or identity data.

6.c — No silent reduction. KRAVIA must not materially reduce agreed safeguards without required notice and a lawful contractual basis. A supplier's certification does not certify Vidyaluma; any certification claim requires its own applicable scope and current evidence.

7. Subprocessors and other recipients

7.a — Authorization. The school authorizes only the processing arrangements properly described in the applicable verified provider schedule and agreed change mechanism. KRAVIA must assess each recipient's role rather than calling every government authority, independent payment party or signing authority a subprocessor by default.

7.b — Flow-down and responsibility. For actual subprocessors, KRAVIA imposes appropriate confidentiality, purpose, security, incident, assistance and deletion duties and oversees their performance. KRAVIA remains

Skip to content

responsible for the performance of its processor obligations; outsourcing is not a blanket disclaimer.

7.c — Changes and objections. Proposed material recipient or location changes receive the notice required by the agreement and law, together with enough information for a meaningful review. A substantiated objection leads to discussion of a suitable alternative, affected-feature restriction or agreed exit remedy. An unreviewed fallback provider may not silently receive private school data.

8. International processing

8.a — India-first direction. Indian storage regions are the preferred direction for school content, not an unverified assertion about every provider, backup or support location. Necessary international processing must be identified and assessed before activation, with applicable safeguards, restrictions and customer disclosures.

8.b — Scope of review. The assessment includes the contracting provider, infrastructure region, subprocessing, remote support, log access, backup destinations and applicable government-access risks. An Indian customer address or local billing currency does not establish that all processing occurs in India.

9. AI and high-risk decisions

9.a — Boundaries. Approved AI may perform a limited authorized task using the minimum necessary school context. Model training on private school content is prohibited. Prompts, embeddings, outputs and logs remain subject to purpose, access, retention and deletion controls, and are not a shared private memory across schools.

9.b — Human control. Final examination marks, official reports and consequential academic outcomes require authorized review. AI must not adjudicate identity, authority, signing, discipline, admissions, medical/psychological status or employment outcomes. T03 supplies the operating restrictions; a school instruction cannot waive an applicable prohibition.

9.c — Assistance and defects. KRAVIA investigates harmful output and attributable processing defects and supports source-grounded correction. The school manages academic appeals and decisions. Necessary safety review must not become unrestricted human access by the AI provider or undisclosed training on reported student conversations.

10. OVSE, DigiLocker and Leegality boundaries

10.a — Adult representatives only. Approved OVSE and DigiLocker onboarding flows concern adult authorized representatives, not student KYC, routine teacher login or attendance. Identity verification and consented document retrieval remain separate from school-authority review.

10.b — Consent and evidence. Each provider transaction needs its required purpose-specific notice and permission. Access is limited to approved claims and documents. Withdrawal, expiry, cancellation and integrity failure must stop the relevant operation; ordinary contract wording is not permission to retain information forbidden by an OVSE or provider condition.

10.c — Signing. Leegality signing is a separate agreement-execution step with document review, signatory capacity and the configured consent method. Signed artifacts and audit trails are protected, integrity-checked and retained only for justified periods. A successful dashboard example is not proof that an application-originated callback and durable record are correct.

11. Rights requests and assistance

Skip to content

11.a — Intake. KRAVIA provides a route for access, correction, restriction, export and deletion requests and promptly routes instructed-school-record questions to the appropriate school contact. Individuals are not required to be subscription purchasers to raise a concern. Identity checks are proportionate to the action.

11.b — Cooperation. KRAVIA provides reasonable technical assistance to locate, correct, export, restrict or delete relevant information and identify recipients. The school responds within applicable timeframes and explains a lawful refusal. Neither party uses the other's involvement as a reason to ignore its own obligations.

11.c — Account deletion. Eligible app-account data is deleted through a genuine request process, available in the app and on the web as required by the product's agreed direction and applicable distribution rules. Any retained school or legal record needs its own justification and restricted access. Account suspension is not substituted for deletion.

12. Personal-data incidents

12.a — Notification and containment. KRAVIA notifies the school without undue delay after identifying a relevant personal-data incident and in time to support applicable deadlines, while independently meeting its own legal and provider duties. Initial notice may be followed by verified updates; complete certainty is not a condition for beginning a required notification.

12.b — Information and cooperation. Available information includes affected services and categories, likely impact, containment, protective steps, relevant contacts and further investigation status. The parties preserve evidence and coordinate notices to individuals and authorities without unnecessary disclosure or a misleading public assurance.

12.c — Responsibility. The school leads notifications for obligations that fall on it; KRAVIA assists and fulfills its own duties. Provider incidents are assessed by actual effect and control. A contract cannot transfer or erase a mandatory regulatory obligation.

13. Audits, assurance and lawful requests

13.a — Assurance. KRAVIA provides appropriate evidence of its relevant processing safeguards, subject to proportionate confidentiality and security restrictions. Where an audit is required, scope, timing and methods must protect other customers and production availability without making a legitimate review impossible.

13.b — Cooperation with authorities. Competent requests are verified, narrowed where appropriate and answered within applicable requirements. The school is informed where permitted. Evidence must not be fabricated, records deleted to avoid review or a regulator redirected solely to a school for KRAVIA's own activities.

13.c — Costs and remedies. Routine contractual assurance and legally required assistance are not subject to surprise fees. Any extraordinary separately chargeable assistance requires prior transparent agreement and cannot obstruct a mandatory right or duty.

14. Return, deletion and end of processing

14.a — Exit. Upon termination, KRAVIA enables an authorized return/export opportunity, with the recorded standard direction of 30 calendar days unless a lawful or agreed extension applies. Records are returned in practical formats within the authorized scope. Other-school records and privileged internal secrets are not included.

Skip to content

14.b — Deletion. Eligible active copies, caches, search indexes, AI retrieval records and provider-held copies are removed under the approved schedule. Restricted backups expire through verified rotation and must reapply

deletion restrictions on restoration. Any retention exception is documented by category, reason, owner and review date.

14.c — Confirmation. Completion evidence identifies the scope and any remaining lawful exceptions or pending provider actions. It must not falsely certify that every copy was instantly erased. Continued retained processing is limited to the justified purpose and remains protected.

15. Contractual remedies and duration

15.a — Liability. The service agreement's expressly agreed valid liability provisions apply according to their scope, with mandatory exceptions preserved. This DPA does not invent a monetary cap, waive child-data rights or deem all privacy losses indirect. Responsibility for subprocessors and independent obligations remains subject to applicable law.

15.b — Survival and amendments. Relevant confidentiality, assistance, retention, dispute and evidence obligations survive termination as needed. Changes require the approved contractual and source-publication process. A portal setting cannot amend this DPA or rewrite an executed copy.

16. Appendix A — Required assurance schedule

16.a — Identity and access. Evidence must cover school-bound server authorization, role and object-level permissions, privileged MFA, session revocation, support access, staff departures and segregation of production and test environments. Tests must include cross-school denial and disputed-authority scenarios.

16.b — Data handling. Evidence must cover encryption/key access, minimal logs, approved data fields, provider egress, anti-malware checks as appropriate, signed-link scope, export authorization, retention jobs, legal holds and deletion propagation. Government-identity data and agreement artifacts have separate access and retention rules.

16.c — Availability and accountability. Evidence must cover incident response, restoration, relevant recovery objectives, provider oversight, change approvals and audit integrity. The recorded governance cadence is quarterly restore testing and an annual disaster-recovery exercise, subject to verified implementation. The accepted school order and approved schedules identify any stronger specific commitments.

Related documents
L01 — Privacy PolicyL02 — Terms & ConditionsL08 — Support & Service Commitments PolicyL10 — Grievance, Complaints & Appeals PolicyT01 — Security & Service Reliability StatementT02 — 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

Skip to content

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 ↑