Data Retention, Export & Deletion Policy

Vidyaluma — A product of KRAVIA PRIVATE LIMITED

Published policy · Effective from 1 November 2026

Approved: 1 November 2026

T07 · Version 1.0.0

Category-specific retention, school exit, individual account deletion, provider cleanup, backups and legal holds.

On this page

1. Purpose and roles
2. Retention schedule and accountable controls
3. School records during the subscription
4. School cancellation and export
5. Individual app-account deletion
6. AI material
7. OVSE and DigiLocker evidence
8. Agreements, payments and legal evidence
9. Public-site analytics and recordings
10. Backups, replicas and providers
11. School closure, ownership change and business transfer
12. Evidence, contact and governance

▶ On this page

1. Purpose and roles

1.a — Operator. This Policy governs retention and disposal of information in Vidyaluma, a product of KRAVIA PRIVATE LIMITED. It distinguishes school-instructed educational records from KRAVIA's own subscription, security, agreement and legal-obligation records. The relevant school and KRAVIA each remain responsible for obligations arising from their actual role.

1.b — No single universal period. Retention depends on category, purpose, legal/contractual duty and a defined start trigger. A period for website analytics is not applied to signed agreements, and a school export window is not the lifetime of every student record. Keeping everything forever or claiming everything disappears instantly is not permitted.

2. Retention schedule and accountable controls

2.a — Schedule. Before a category is activated, the approved schedule identifies its data, purpose, owner, start trigger, active retention, archive/backup handling, deletion method, recipients and any lawful exception. Undefined schedules are review blockers, not permission for indefinite retention. The actual schedule must be supported by operational tests and applicable legal analysis.

2.b — Minimum necessary record. Prefer a permitted status, reference or bounded audit event over a complete raw document where that is sufficient. Hashes, pseudonymous identifiers and transaction references may still identify a person and need protection. A hash is not automatically anonymous or a reason to ignore a deletion request.

2.c — Review. Owners review retention on material changes and at least through annual governance. Overdue deletions, failed jobs and unresolved provider cleanup are tracked to completion. A successful deletion-job invocation is not proof that all intended records were removed.

3. School records during the subscription

3.a — Instructed use. Relevant academic, attendance, staff, guardian, communication, fee and document records are retained for the authorized school function and applicable instructions. The school must identify educational recordkeeping duties and avoid unnecessary categories. KRAVIA must not use active subscription status as a reason to keep unrelated temporary data.

3.b — Corrections and history. Authorized corrections preserve necessary provenance and distinguish original, superseded and approved records. History is limited to justified audit and dispute purposes, not made available to every user indefinitely. KRAVIA fixes attributable software faults while the school approves academic changes.

3.c — Individual rights. An individual may request access, correction, export or deletion while the school remains active. The relevant purpose and lawful retention are assessed separately. A blanket "the school owns all data" answer is insufficient, and an account being school-managed does not remove KRAVIA's own duties.

4. School cancellation and export

4.a — Standard recorded window. After subscription termination, the recorded policy direction is a 30-calendar-day opportunity for an authorized school to request and download its eligible records. The actual termination date and deadline are communicated. Any mandatory or specifically agreed extension applies, including appropriate handling of an inaccessible or failed export path.

4.b — Export scope. Exports should include authorized student, staff, academic, attendance, fee and relevant document records in practical formats, with schema or field explanations when needed. Third-party licensed content, another school's records, reusable credentials and protected internal security material are not included indiscriminately.

4.c — Secure delivery. Current school authority is verified before an export. Delivery is restricted, expiry-controlled where appropriate and auditable. The school is told about remaining access and deletion plans. Non-payment or a school dispute is not automatic authority to deny every lawful privacy/export request.

4.d — After the window. The school receives appropriate advance deletion information, expired access is restricted and eligible records enter the approved disposal schedule. The export window does not silently become an unlimited archive or a promise to erase all legally required records on day 31. Exact category/backup periods must be confirmed before publication.

Skip to content

5. Individual app-account deletion

5.a — Initiation. Users must have a discoverable in-app request route and an external public web route at /privacy-request, without reinstalling the app. Email assistance at support@vidyaluma.in remains an alternative for a failed or inaccessible form. A current school work email or paid account is not universally required.

5.b — Scope and verification. We verify the person or appropriate representative proportionately, identify associated account information, disable unnecessary further processing and delete eligible data. Linked memberships and a child's guardian authority require careful review. A request must not expose another person's account existence or protected records.

5.c — Retained records. A school academic record, executed adult agreement, financial record or scoped security evidence may require separate lawful retention. We explain the category, reason and applicable period or criteria and restrict access. Temporary deactivation, freezing or removal of a login is not represented as account/data deletion.

6. AI material

6.a — Inputs and temporary processing. Raw prompts, extracted content, temporary scans and intermediate outputs are minimized and removed when their authorized task no longer requires them, under the confirmed schedule. They must not enter unrestricted debugging or model-training stores. Provider no-training and retention terms are separately verified.

6.b — Approved outputs. A teacher-approved report or mark follows the relevant school-record schedule rather than the temporary-prompt schedule. A draft, rejected output or safety report may have a different short justified lifecycle. Review evidence is minimized and access-limited.

6.c — Retrieval and memory. Deletion or source revocation applies to relevant embeddings, retrieval indexes, cached context and private conversation memory. Tests must check that a deleted record cannot still be retrieved through a semantic search or restored conversation. Cross-school private memory is prohibited.

7. OVSE and DigiLocker evidence

7.a — Minimal outcomes. Approved adult-representative verification retains only the necessary permitted status, references, timestamps and bounded evidence. Full Aadhaar numbers, unnecessary raw identity payloads, provider passwords, OTPs and access tokens must not be retained as ordinary audit material.

7.b — Temporary documents and consent. DigiLocker documents and temporary provider data are used only for the approved consented onboarding task and removed when no longer necessary or permitted. Withdrawal stops further consent-dependent access. Stricter provider and OVSE consent/deletion conditions prevail over a generic desire to retain audit evidence.

7.c — Failed or disputed checks. Cancellation, failure, mismatch and rejected onboarding need a separate minimal retention rule. Necessary dispute evidence is scoped and protected. Keeping a complete identity file for every failed attempt indefinitely is not justified by this Policy.

8. Agreements, payments and legal evidence

8.a — Signed agreements. Leegality-signed agreements, certificate information and relevant audit trails are protected for the justified contractual/evidentiary period. The period must be approved against actual obligations and limitation needs. A disputed document is preserved unchanged; it is not silently replaced by a corrected contract.

Skip to content

8.b — Financial records. Invoices, credit notes, tax records, refunds and reconciliation evidence are kept for the applicable verified financial/legal retention period. We do not collect or retain bank passwords, card security codes or Aadhaar signing OTPs to support billing records. School-fee records and KRAVIA's own subscription accounts have separate roles.

8.c — Legal holds. A competent order, active dispute or other justified obligation may suspend deletion of specifically relevant material. The hold identifies its authority, scope, owner and review trigger. It must not become an indefinite hold over every school's information. Normal disposal resumes when the reason ends.

9. Public-site analytics and recordings

9.a — Recorded ceilings. The proposed maxima are 30 days for permitted public-site session recordings and 14 months for identifiable visitor analytics. Earlier deletion applies where necessary. These ceilings require operational confirmation and do not authorize tools or sensitive routes prohibited by L03.

9.b — Withdrawal. New optional tracking stops upon withdrawal. Controllable optional cookies/storage are cleared and retained identifiable information is assessed for deletion or restriction. The inability to identify a genuinely anonymous aggregate differs from a provider's failure to support an identifiable deletion.

9.c — Separate logs. Justified security logs and legal evidence follow their approved category-specific requirements. They cannot be repurposed as visitor marketing profiles or used to re-create information that was deleted from optional analytics.

10. Backups, replicas and providers

10.a — Active copies. Approved disposal includes relevant primary databases, replicas, object stores, exports, search/index caches, mobile caches where controllable and AI processing stores. Scope and failures are recorded. Simply hiding a row from the interface does not establish deletion.

10.b — Restricted backups. Backups follow a verified rotation schedule and remain access-restricted. Where immediate per-record removal is not technically supported, the retained backup is not used for unrelated processing and expires within the approved period. Restore procedures must reapply deletion and access restrictions before restored data returns to service.

10.c — Providers. KRAVIA requests appropriate deletion/return from relevant processors, revokes unnecessary tokens and obtains available evidence. A completion notice must disclose outstanding lawful exceptions or pending provider actions rather than falsely claim universal erasure.

11. School closure, ownership change and business transfer

11.a — School changes. A closure, merger or ownership transfer requires verified legal authority and appropriate arrangements for student records. New administrators do not automatically acquire another school's records or authority over every individual's rights. Protected transfer and restricted retention may be necessary while disputes are resolved.

11.b — Vidyaluma discontinuation. Permanent shutdown requires notice, workable exports, relevant prepaid-service remedies and lawful deletion/retention. A business acquisition does not remove purpose restrictions or authorize sale of student profiles. Appropriate recipients and individuals receive required information.

12. Evidence, contact and governance

Skip to content

12.a — Completion evidence. Deletion/export records identify the request, authorized scope, date, actions, relevant providers and remaining exceptions. Logs are minimal and protected. They should not preserve the deleted record's full content merely to prove it once existed.

12.b — Contact and appeal. Use /privacy-request or support@vidyaluma.in. Explain the record or account and safe references. Refusals and unresolved cleanup can be escalated under L10. Applicable deadlines, rights and enforceable obligations are not replaced by an internal target.

12.c — Publication. Retention schedules and their implementation evidence remain subject to verified operational review. Period changes need review and appropriate notice. The Policy and public history are read-only through all product surfaces and change only through authorized source releases.

Related documents
L01 — Privacy PolicyL02 — Terms & ConditionsL03 — Cookie & Tracking Technologies PolicyL07 — Billing, Subscription, Cancellation & Refund PolicyL09 — Data Processing AgreementL10 — Grievance, Complaints & Appeals PolicyT01 — Security & Service Reliability StatementT02 — Student & School Data Protection NoticeT03 — Responsible AI PolicyT06 — Subprocessor & International Processing Notice

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
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

Legal
Privacy Policy
Terms & Conditions
Cookie & Tracking Technologies Policy
Acceptable Use Policy
Disclaimer
Accessibility Statement

Skip to content

Subprocessor & International Processing Notice

Data Retention, Export & Deletion Policy

Vulnerability Disclosure Policy

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.