School Control, Access & Sharing Statement

Vidyaluma — A product of KRAVIA PRIVATE LIMITED

Published policy · Effective from 1 November 2026

Approved: 1 November 2026

T05 · Version 1.0.0

School-scoped authority, account lifecycle, report sharing, disputes and individual rights.

On this page

1. School control is bounded authority
2. Roles, membership and least privilege
3. Account lifecycle and recovery
4. Ownership, merger and closure disputes
5. Reports and document sharing
6. Corrections, approval and history
7. Student, guardian and staff privacy
8. Exports, exit and data deletion
9. Policy immutability and assistance

▶ On this page

1. School control is bounded authority

1.a — Product. Vidyaluma, a product of KRAVIA PRIVATE LIMITED, enables authorized people to perform their school's permitted tasks. Administrative control is scoped by school, role, data and action. It is not unlimited ownership of personal information or permission to override legal rights.

1.b — Responsibilities. Schools identify appropriate representatives and educational decision-makers. KRAVIA supplies and must enforce the relevant server-side access, revocation, correction and audit mechanisms. A school selecting a role does not excuse a defect that exposes another school's information.

2. Roles, membership and least privilege

2.a — Assignment. Access is based on verified school membership and necessary responsibilities, not a role label alone. Teachers, guardians, students, finance staff and administrators should receive only the relevant

records and actions. Multi-school membership is evaluated independently for each school.

2.b — Protected actions. Exports, account recovery, guardian changes, permission grants, payment actions and signing transitions need appropriate authorization and safeguards. A hidden button or user-controlled school identifier is not security. Bulk actions require the same scope checks as individual actions.

2.c — Review. Schools review access when roles change and report unauthorized use. KRAVIA manages its employee and infrastructure privileges independently and cannot make every support employee a school super-administrator by default.

3. Account lifecycle and recovery

3.a — Creation. School-managed invitations or authorized provisioning establish access for students, parents and staff. The correct school and guardian association must be verified. An invitation must not expose protected records before the recipient's relevant authority is established.

3.b — Departures. When staff leave or permissions end, the school must promptly initiate the change and KRAVIA's controls must revoke relevant roles and sessions. Handover transfers responsibilities without sharing former users' credentials or silently reassigning their personal acceptance/signing history.

3.c — Compromise. Recovery uses proportionate verified methods, revokes compromised access and records the action. High-risk administrator recovery requires stronger review. Public biographical information, an Aadhaar match or access to an old phone number does not by itself establish current school authority.

4. Ownership, merger and closure disputes

4.a — Competing claims. Where two parties claim school authority, sensitive changes may be frozen while evidence is reviewed independently. Restrictions should protect records and avoid unnecessary disruption to safe school operations. Neither party's model-generated explanation is decisive proof.

4.b — Legal transition. A school closure, merger or ownership transfer requires verified authority and a clear lawful destination for relevant records. The change must not automatically grant a new entity access to unrelated data or retroactively rewrite agreement signatories.

4.c — Evidence. Necessary authority, access and decision records are preserved with restricted visibility. Review cannot override failed integrity, withdrawn consent or missing provider permission. A disputed signature is investigated under L10 rather than replaced in storage.

5. Reports and document sharing

5.a — Scope. A school shares an approved view or document, not unrestricted workspace access. Recipient identity or relationship, purpose, selected records and sensitivity determine the safeguards. Teacher or parent access must not expose unrelated pupils or another family's details.

5.b — Links and expiry. Where sharing links are supported, they require appropriate unpredictability, access scope, expiry and revocation. Sensitive records may require recipient verification beyond possession of a URL. Tokens must not be logged by analytics, exposed in public search or treated as harmless query parameters.

5.c — Copies. A downloaded, printed or onward-shared copy may not be technically revocable. The school should explain recipient responsibilities and use an appropriate sharing method before disclosure. This limitation must not be hidden by a blanket claim that every document can always be recalled.

Skip to content

6. Corrections, approval and history

6.a — Academic changes. Authorized school personnel verify and approve marks, attendance and report corrections. KRAVIA investigates attributable software faults and provides secure correction mechanisms. Approved records and earlier versions must remain distinguishable where history is justified.

6.b — AI drafts. AI may assist authorized preparation but cannot publish consequential outcomes without meaningful human approval. The reviewer, relevant sources and material changes are recorded. An automatically checked approval field is not an adequate substitute for actual review.

6.c — Appeal. Students and guardians may challenge academic accuracy through the school and report technical or privacy concerns to KRAVIA. Good-faith appeals do not justify retaliatory restrictions. The responsible party and available remedy must be identified.

7. Student, guardian and staff privacy

7.a — Individual requests. The school-first handling of educational records does not remove individual rights or KRAVIA's own duties. /privacy-request and the in-app deletion route must remain usable as appropriate. A person without a work email or subscription may still ask about their information.

7.b — Sensitive relationships. Guardianship restrictions, parent conflicts, adulthood and transfers require a specific review before protected disclosure. An administrator must not resolve such issues by indiscriminately merging accounts or sharing credentials.

7.c — Monitoring and support. Authorized support and safeguarding access is limited to a justified task. School control does not mean unrestricted access to every private AI conversation, a child's location or staff device activity. Access and retention boundaries must be explained.

8. Exports, exit and data deletion

8.a — Authorized export. The school may export its permitted student, staff, attendance, academic, fee and relevant document records in practical formats. The standard recorded exit direction is a 30-calendar-day opportunity after termination, with necessary extensions. The export must exclude other-school data and protected internal secrets.

8.b — Verification. Export and transfer actions require current authority, protected delivery and audit evidence. An unpaid balance does not automatically remove privacy rights, and an ownership dispute does not justify handing records to the first claimant.

8.c — Deletion. T07 governs category-specific cleanup, backups and legal holds. Account revocation is not deletion. The school cannot instruct the destruction of material subject to a valid legal hold, while KRAVIA cannot claim an indefinite hold over the entire database without a specific reason.

9. Policy immutability and assistance

9.a — No policy editor. School, owner, Founder and internal administrators cannot modify, upload replacements for, publish or delete Legal/Trust documents through product interfaces or application APIs. Configuring a school workflow does not amend the agreement or policy body. Revisions require the approved source-release process.

9.b — Help. Contact support@vidyaluma.in for access, recovery or sharing assistance. Sensitive action requires proportionate verification; a general concern may be received without access to protected records. Disputes and

Skip to content

complaints use L10 and do not remove mandatory external remedies.

Related documents
L01 — Privacy PolicyL02 — Terms & ConditionsL09 — Data Processing AgreementL10 — Grievance, Complaints & Appeals PolicyT01 — Security & Service Reliability StatementT02 — Student & School Data Protection NoticeT03 — Responsible AI PolicyT07 — Data Retention, Export & Deletion Policy

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

Skip to content

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.