# Acceptable Use Policy

**Vidyaluma** — A product of KRAVIA PRIVATE LIMITED

Published policy · Effective from 1 November 2026

Approved: 1 November 2026

L04 · Version 1.0.0

Authorized educational use, prohibited conduct, user-content safety, investigation and fair enforcement.

**On this page**

1. Application and principles
2. Accounts and access
3. Educational records and personal information
4. Child safety and communications
5. AI-specific restrictions
6. Intellectual property and service limits
7. Investigation and enforcement
8. Cooperation, contact and changes

▶ On this page

## 1. Application and principles

**1.a — Scope.** This Policy governs authorized use of Vidyaluma, a product of KRAVIA PRIVATE LIMITED, including school accounts, public request channels, communications, document processing and enabled AI tools. It supplements the school agreement and L02 without converting a child into a contracting purchaser.

**1.b — Responsible use.** Use the service only for a lawful, authorized school or service purpose. Respect other people's privacy, safety and intellectual property. A school's permission does not authorize misuse of another school, unlawful discrimination, disclosure of protected information or circumvention of a person's rights.

## 2. Accounts and access

**2.a — Identity and authority.** Do not impersonate a student, guardian, employee, signatory or government authority; forge school authority; share privileged credentials; or access an account after your authorization ends. A legitimate role in one school grants no rights over another school's data.

**2.b — Technical misuse.** Attempts to defeat authorization, exploit another user's session, scrape protected records, introduce malware, steal credentials, bypass billing controls or disrupt availability are prohibited. Automated access requires an approved interface, appropriate permission and compliance with limits. Researchers must follow T08 rather than treating this Policy as blanket testing authorization.

**2.c — Recovery and support.** Do not submit false recovery evidence, manipulate support staff to obtain access or use identity/signing workflows on behalf of an unaware person. Report suspected compromise promptly. KRAVIA remains responsible for maintaining secure recovery controls rather than relying only on user vigilance.

# 3. Educational records and personal information

**3.a — Lawful inputs.** Upload only records you are authorized to provide, use relevant fields and identify the correct school and person. Do not falsify marks, attendance, fee records, guardian relationships, signatures or audit evidence. Corrections must use the authorized process and preserve an appropriate history.

**3.b — Restricted data.** Do not send Aadhaar numbers, identity payloads, health records, passwords, OTPs, private report links or signing credentials through general AI prompts or public enquiries. A protected workflow must state what it needs and provide an authorized channel. Data available in a provider account must not be retrieved merely out of curiosity.

**3.c — Sharing.** Share reports only with authorized recipients for the stated purpose. Do not publish student records, expose another family's contact information, trade school databases or use screenshots to bypass access restrictions. Recipient access and appropriate permission must be checked before using student photographs or achievements publicly.

# 4. Child safety and communications

**4.a — Prohibited content.** Child sexual exploitation, grooming, sexual solicitation of minors, credible threats, stalking, discriminatory harassment, bullying, doxxing, fraud and encouragement of dangerous wrongdoing are prohibited. Do not use school messaging to arrange secret or unauthorized adult-child contact.

**4.b — Reporting and safeguarding.** Users must have an appropriate way to report concerning content and, where relevant, block contact. Schools manage educational safeguarding duties; KRAVIA handles platform reports, attributable defects and applicable reporting obligations. Necessary evidence is restricted and preserved, not circulated in public groups.

**4.c — Urgent danger.** Vidyaluma is not a replacement for emergency responders or direct school safeguarding contact. Seek appropriate immediate help when someone is in danger. This boundary does not excuse failure of a safety-related function that KRAVIA has expressly undertaken to provide.

# 5. AI-specific restrictions

**5.a — Permitted assistance.** Authorized AI use must follow T03 and the relevant task purpose. Do not publish consequential AI-generated marks, reports or recommendations without the required human review, or present an AI draft as a verified official record.

**5.b — Prohibited processing.** Do not use Vidyaluma AI to identify faces, infer children's emotions, diagnose medical or psychological conditions, adjudicate identity, determine guilt, autonomously reject admissions or make employment decisions. Attempts to retrieve other-school context or bypass safety controls are prohibited.

**5.c — Content and tools.** Do not generate fabricated citations, forged credentials, deceptive official documents or harmful instructions. Do not authorize an agent to send messages, change records, approve payments or

execute an agreement outside the approved human-controlled process. User instructions do not override server-side authority checks.

# 6. Intellectual property and service limits

**6.a — Content rights.** Respect copyright, licenses and confidential materials. Uploading a textbook or question bank requires appropriate rights. AI output is not guaranteed to be original, exclusive or free of third-party rights. Content complaints can be submitted under L10 without publishing protected material.

**6.b — Commercial misuse.** Do not resell unauthorized access, manipulate subscription limits, introduce unexpected chargeable operations or use school contact information for unrelated marketing. Lawful interoperability or other rights that cannot be excluded are preserved; contact support about an authorized integration instead of bypassing safeguards.

# 7. Investigation and enforcement

**7.a — Proportionate response.** KRAVIA may investigate a credible report, preserve necessary evidence, restrict offending content or accounts, require remediation, or suspend affected functions according to severity, confidence and risk. Less disruptive measures should be considered. Ordinary mistakes are distinguished from repeated or deliberate abuse.

**7.b — Fair process.** Where safe and lawful, affected parties receive the reason, relevant scope and an opportunity to respond. Urgent containment may precede notice. There is no automatic permanent ban based solely on an AI classifier, unverified allegation or good-faith complaint against Vidyaluma.

**7.c — Appeals and exit.** Appeals follow L10 with an appropriately independent reviewer. Suspension does not silently authorize destruction of educational records or blanket denial of rights requests. Lawful export, preservation and deletion rules remain applicable, subject to necessary security restrictions.

# 8. Cooperation, contact and changes

**8.a — Cooperation.** Schools should notify KRAVIA of departing staff, material misuse and compromised access. KRAVIA must investigate attributable product failures and assist with lawful corrections. Each party remains accountable for its own acts and obligations; this Policy does not transfer all misuse liability to a school or child.

**8.b — Contact.** Report misuse through the available in-product reporting route or support@vidyaluma.in. Submit a concise account of the issue and safe references. Sensitive evidence requires a protected collection method. Updated rules require the controlled approval and publication process, not an editable portal announcement.

**Related documents**
L02 — Terms & ConditionsL10 — Grievance, Complaints & Appeals PolicyT02 — Student & School Data Protection NoticeT03 — Responsible AI PolicyT05 — School Control, Access & Sharing StatementT08 — Vulnerability Disclosure Policy

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

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 ↑