# Support & Service Commitments Policy

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

Published policy · Effective from 1 November 2026

Approved: 1 November 2026

L08 · Version 1.0.0

Support ownership, incident handling, maintenance, availability, service remedies and continuity.

**On this page**

1. Service scope and commitments
2. Contact and secure intake
3. Severity and prioritization
4. Investigation and responsibilities
5. Availability and maintenance
6. Provider failures and safe fallback
7. Backups, recovery and continuity
8. Remedies and closure
9. Discontinuation and governance

▶ On this page

## 1. Service scope and commitments

**1.a — Provider.** KRAVIA PRIVATE LIMITED provides Vidyaluma support for the contracted platform and its own integrations. Schools remain responsible for their educational administration and for identifying authorized support contacts. Students, parents and other affected people may still raise privacy, safety or accessibility concerns directly through an appropriate route.

**1.b — Targets versus guarantees.** This Policy establishes the support process. Specific staffed hours, response times, uptime percentages, recovery objectives and credit formulas must be stated in an approved service schedule before being promised. No 24-hour staffed service, zero-loss recovery or 100% uptime guarantee is created by a general use of the word "enterprise".

## 2. Contact and secure intake

Skip to content

**2.a — Channels.** Use the available in-product support route, the main website's contact page or support@vidyaluma.in. Give the school, affected service, safe reference, time and impact. A protected privacy request can start at /privacy-request. Submitting a report must not require public disclosure of a student record or identity document.

**2.b — Acknowledgement.** A successfully stored request receives a reference and a useful next step. The interface must not display receipt before the server has actually accepted the request. If a form or dependency fails, the alternative contact route remains visible and the failed submission is not silently discarded as completed.

**2.c — Verification.** Verification is proportionate to the requested action. Anyone may describe a concern; disclosure, access change, payment action or export requires appropriate authority. Support must not ask for account passwords, Aadhaar OTPs, API secrets or full card credentials.

# 3. Severity and prioritization

**3.a — Critical.** Suspected cross-school exposure, widespread authentication failure, material data corruption or a major outage affecting critical operations receives urgent assessment and security escalation where relevant. A child's immediate danger is also directed to appropriate emergency and school safeguarding channels; Vidyaluma does not replace them.

**3.b — High.** A substantially blocked school workflow, failed verification/signing process or a serious accessibility barrier without a reasonable alternative receives priority based on actual impact. The reviewing team may adjust severity with reasons; commercial pressure alone must not suppress a genuine security report.

**3.c — Normal and improvement.** Isolated errors with a workaround, usage questions and nonurgent improvements are tracked in the relevant queue. A feature request is not automatically a binding delivery promise. The support record distinguishes acknowledgement, work in progress, pending information, resolved and reopened states.

# 4. Investigation and responsibilities

**4.a — KRAVIA work.** KRAVIA investigates attributable software, integration, permissions, processing and delivery defects. It maintains a responsible owner, seeks safe reproducible evidence, communicates material developments and provides an appropriate correction or remedy. Outsourced hosting or AI does not remove these responsibilities.

**4.b — School cooperation.** The school supplies accurate non-sensitive context, identifies affected workflows and authorizes protected actions through an appropriate representative. It remains responsible for academic reassessment and decisions. Delays caused by missing necessary information are recorded and explained rather than treated as unlimited permission to stop work.

**4.c — Controlled access.** Employee access to school data is restricted, justified, time-bounded where appropriate and audited. A support request is not blanket permission to impersonate users, browse unrelated records or share production content with a general AI tool.

# 5. Availability and maintenance

**5.a — Measurement.** Availability reports must reflect measured services, defined periods and verified incidents. A webpage loading does not prove its enquiry, authentication or policy data is working. Status must not default to operational when the monitoring source is unavailable.

**Skip to content**

**5.b — Planned maintenance.** We seek lower-impact windows and provide appropriate advance notice of expected disruption, affected functions and any preparatory action. The exact notice interval follows the agreed schedule; this Policy does not invent a universal interval. Material overruns require updated communication.

**5.c — Emergency work.** Urgent patches and infrastructure repairs may occur without advance notice where delay creates material risk. KRAVIA communicates as soon as practicable, preserves incident/change evidence and verifies the recovery rather than declaring success after a restart alone.

# 6. Provider failures and safe fallback

**6.a — External dependencies.** KRAVIA coordinates with relevant providers, explains user impact and takes reasonable mitigation measures. A provider outage must not create duplicate payments, incorrectly approved identity results, fabricated signing success or publication of incomplete AI reports.

**6.b — Onboarding and AI.** Failed OVSE, DigiLocker or Leegality steps remain pending until the mandatory checks succeed through an approved route. AI work may be paused or offered an authorized non-AI alternative; a fallback provider must itself be reviewed before receiving school content.

**6.c — User expectations.** We explain limitations, realistic next steps and what evidence remains outstanding. Internal test success, queued retries and a provider dashboard transaction are not represented as completed production customer journeys.

# 7. Backups, recovery and continuity

**7.a — Recovery planning.** Critical services require documented backup, restore and continuity procedures. The recorded governance direction is quarterly restore tests and an annual disaster-recovery exercise. Actual tested recovery-time and recoverable-data-loss objectives must be defined per service and supported by evidence before being guaranteed.

**7.b — Safe restoration.** Restored data must preserve tenant boundaries, valid authority, legitimate records and deletion/legal-hold rules. We must not reset production to an empty state, delete authentic audit history or bypass validation simply to make a health indicator green.

**7.c — School continuity.** Schools should maintain appropriate operational fallback procedures for critical activities. KRAVIA provides relevant information and authorized exports or recovery assistance within its commitments. This shared preparation does not excuse a contracted reliability or backup failure.

# 8. Remedies and closure

**8.a — Remedies.** Verified failures may justify a correction, service credit, subscription extension, eligible refund or other remedy under the accepted agreement and applicable law. A service credit is not automatically the exclusive remedy for every confidentiality, data-loss or legally protected claim.

**8.b — Closure.** Resolution requires evidence that the issue or agreed outcome is addressed, relevant user communication and any remaining corrective actions. A ticket may be reopened when the same problem persists. Security incidents require the additional evidence and review in T01.

**8.c — Escalation.** Unresolved support, accessibility, billing or conduct complaints use L10. Schools may request a review by an appropriately independent person. No one must give up a statutory complaint right to obtain routine technical assistance.

# 9. Discontinuation and governance

Skip to content

**9.a — Permanent exit.** A decision to discontinue Vidyaluma requires appropriate advance notice, a workable export opportunity, handling of eligible unused prepaid service and a lawful retention/deletion plan. Extraordinary events require reasonable mitigation and communication rather than an automatic indefinite suspension of responsibility.

**9.b — Publication accuracy.** Public claims reflect actual staffed coverage and capabilities. This Policy and any service schedule are reviewed on material change and at least annually. Changes require authorized approval and controlled source deployment; no administrator or automated agent may edit commitments through the website.

**Related documents**
L02 — Terms & ConditionsL06 — Accessibility StatementL07 — Billing, Subscription, Cancellation & Refund PolicyL10 — Grievance, Complaints & Appeals PolicyT01 — Security & Service Reliability StatementT07 — Data Retention, Export & Deletion Policy

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
Subprocessor & International Processing Notice

**Legal**
Privacy Policy
Terms & Conditions
Cookie & Tracking Technologies Policy
Acceptable Use Policy
Disclaimer
Accessibility Statement
Billing, Subscription, Cancellation & Refund Policy
**Support & Service Commitments Policy**

Skip to content

Data Retention, Export & Deletion Policy

Vulnerability Disclosure 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 ↑