Cookie & Tracking Technologies Policy

Vidyaluma — A product of KRAVIA PRIVATE LIMITED

Published policy · Effective from 1 November 2026

Approved: 1 November 2026

L03 · Version 1.0.0

Necessary storage, optional measurement, consent and tracking boundaries on Vidyaluma websites and apps.

On this page

1. Purpose and scope
2. Necessary technologies
3. Optional analytics
4. Heatmaps and session recordings
5. Consent preferences and withdrawal
6. Retention and tracking inventory
7. Mobile and child-facing boundaries
8. Contact and changes

▶ On this page

1. Purpose and scope

1.a — Product. This Policy applies to cookies, browser storage, pixels, SDK identifiers and similar technologies used in connection with Vidyaluma, a product of KRAVIA PRIVATE LIMITED. It distinguishes the public marketing website from authenticated school, identity, signing and mobile experiences. The presence of a technology in one surface does not authorize it in another.

1.b — Relationship to privacy. L01 explains the wider use of personal information. Consent to optional measurement is not subscription acceptance, parental consent, signing consent or permission to access a government identity service. Those decisions require their own appropriate information and controls.

2. Necessary technologies

Skip to content

2.a — Essential operation. Necessary technologies may maintain a signed-in session, protect against abuse, remember a user's consent choices, secure a request or support a user-selected feature. They must be limited to

that purpose and retained no longer than justified. Calling a tool "essential" does not make promotional attribution, session replay or general audience analytics necessary.

2.b — Security and third parties. An anti-abuse or identity provider may process limited technical information when a protected transaction is initiated. The actual recipient, data, storage and purpose must be assessed and disclosed. Essential processing must not silently include optional advertising modules or tracking on every page merely because a provider is installed.

2.c — Local storage. Necessary preferences and authentication material require appropriate protection and expiration. Sensitive educational records, signing links, passwords and identity payloads must not be placed in browser storage for analytics convenience. Offline school records have a separate controlled protection and cleanup policy.

3. Optional analytics

3.a — Choice before activation. Optional website analytics must remain inactive until the visitor gives an affirmative, informed choice. Rejection must be readily available and must not be disguised by color, wording or unnecessary steps. Scrolling, continuing to browse or closing a banner is not treated as acceptance of optional tracking.

3.b — Limited use. Permitted visitor measurement may help understand page performance, navigation and service interest. It must exclude student records, contact-message contents, identity documents, payment details and secrets. Collection must be the minimum needed for the disclosed purpose, without building an unrelated commercial profile of a student or school user.

3.c — Providers. Google Analytics or any alternative is not authorized solely because this Policy names an example. The specific deployment must appear in the verified technology inventory, match the consent category and satisfy applicable privacy and transfer review. This Policy does not claim that a named analytics service is currently installed.

4. Heatmaps and session recordings

4.a — Narrow scope. Session replay and identifiable interaction recording are not permitted in authenticated school portals, child-facing apps, privacy-request forms, identity verification, signing or payment flows. Any approved public marketing-page deployment requires explicit optional consent, a page allowlist and a documented reason that less intrusive aggregate measurement is insufficient.

4.b — Capture restrictions. Recording must exclude sensitive routes and elements at the source. Passwords, form values, uploaded files, private links, query-string secrets and student information must never be recorded. Masking is tested against actual network payloads and rendered dynamic fields; a dashboard setting alone is not evidence that capture is safe.

4.c — Access and retention. Access is restricted to authorized analysts for the stated improvement purpose. The recorded proposed ceiling is 30 days, with earlier deletion when justified. Recordings must not be used to identify a visitor across products, assess a child, train a model or monitor an employee's private activity.

5. Consent preferences and withdrawal

5.a — Banner choices. The public website provides understandable Accept, Reject and Customize choices. Necessary categories are explained separately; optional categories are off by default. A persistent Cookie preferences control allows a visitor to change the choice without creating an account or contacting sales.

Skip to content

5.b — Withdrawal. Withdrawal must stop new optional collection and applicable SDK activity without waiting for the next visit. It does not retroactively undo a lawful past operation, but retained identifiable information is separately assessed for deletion or restriction. We clear controllable optional storage and propagate appropriate requests to relevant providers.

5.c — Preference evidence. A limited consent record may retain the choice, notice version, relevant time and technical preference reference. It must not become an advertising identifier. Choices can differ across devices or browsers; the interface must explain when a choice is local rather than pretending that it controls every device automatically.

6. Retention and tracking inventory

6.a — Retention ceilings. The recorded proposed maximum for identifiable public-site analytics is 14 months; it is not an obligation to retain information that long. The 30-day replay ceiling and 14-month analytics ceiling do not apply as a blanket deletion rule to justified security or contractual records. T07 governs those separate categories and required legal holds.

6.b — Required inventory. Before activation, every technology must have a recorded name, provider, affected route/app, purpose, consent category, data collected, first/third-party status, lifetime and relevant processing location. Material changes require review and renewed consent where needed. The production inventory must describe real cookies and SDKs, not sample names copied from a generator.

6.c — Unknown or noncompliant tools. A new or unclassified tracker remains disabled until reviewed. If a tool collects before consent, ignores rejection or cannot exclude sensitive information, it must be blocked and investigated. We do not fix that behavior by silently relabeling the tool as necessary.

7. Mobile and child-facing boundaries

7.a — Mobile collection. App SDK collection is assessed separately from browser cookies and must match the app's actual privacy disclosures and store declarations. Permission denial, logout and deletion behavior must be tested. Installing a web consent banner does not control a mobile SDK unless the integration actually enforces that choice.

7.b — Children. We prohibit student-data advertising, sale and unrelated commercial profiling. Child-targeted experiences require the relevant audience, identifier, SDK and platform safeguards. Adult transport tracking or representative signing is not authority to collect child-device location or biometrics.

8. Contact and changes

8.a — Assistance. Use Cookie preferences for immediate changes, /privacy-request for a related rights request, or support@vidyaluma.in for assistance. A visitor may ask about a technology without purchasing a subscription. Avoid sending private cookies, session tokens or full diagnostic dumps in ordinary email.

8.b — Publication control. This Policy and its verified inventory are versioned through approved source releases. No website, app, administrator or provider dashboard may silently rewrite the published policy. A new version must carry real publication details and appropriate notice; the intended October date does not authorize historical tracking.

Related documents
L01 — Privacy PolicyT02 — Student & School Data Protection NoticeT06 — Subprocessor & International Processing NoticeT07 — Data Retention, Export & Deletion Policy

Skip to content

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

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 ↑