

Data Compliance

Last updated: July 1, 2026

This page describes how EduPilot approaches data protection compliance across our web platform and mobile applications, and complements the detail in our Privacy Policy and Terms & Conditions.

01

Regulatory alignment

EduPilot processes personal data in alignment with India's Digital Personal Data Protection Act, 2023 (DPDP Act), including its provisions on consent, purpose limitation, and additional safeguards for processing children's personal data.

Because most ward (student) data belongs to minors, consent for ward data flows through a verifiable parent/guardian relationship or the enrolling school acting on parents' behalf, rather than the student directly.

This page describes our compliance posture at a program level; the legal basis for any specific school's use of the Platform is also governed by that school's own enrollment and consent agreements with parents.

02

Data localization

Production data is hosted with cloud infrastructure providers operating data centers serving the Indian market, consistent with data-residency expectations for institutional and student records.

Where a sub-processor operates outside India (for example, for specific analytics or communication tooling), transfers are limited to what's necessary for that function and governed by contractual safeguards with the vendor.

03

Web application compliance

TLS encryption in transit for all web traffic between browsers and our servers.

Role-based access control enforced server-side, so a parent, teacher or administrator session can only query data scoped to their role and linked wards.

Session and cookie handling limited to strictly necessary authentication cookies plus aggregated, non-identifying product analytics — detailed further in our Privacy Policy.

04

Mobile application compliance

Our iOS and Android apps request only the device permissions required for core functionality (e.g., notifications for diary/fee alerts, camera access only if a user chooses to upload a document or photo). We do not request background location or contact-list access.

App store disclosures — Apple's Privacy Nutrition Label and Google Play's Data Safety section — are kept in sync with the categories of data actually collected by the mobile app, as described in our Privacy Policy.

Push notification tokens and device identifiers are used solely for delivering platform notifications (fee reminders, diary entries, exam results) and are not shared with third-party advertising networks.

05

Payment data compliance

Fee payment features integrate with PCI-DSS compliant payment gateway partners. Full card, UPI credential or bank details are captured and processed directly by the gateway — EduPilot's servers do not store raw payment instrument data.

06

Breach notification

In the event of a data breach affecting personal data on the Platform, we will notify affected schools without undue delay, and will notify affected individuals and relevant regulators where required under applicable law.

07

Vendor & sub-processor due diligence

Infrastructure, payment gateway, and communication (SMS/email/push) sub-processors are reviewed for their own security and compliance posture before integration, and are bound by contractual data protection terms.

A current list of key sub-processor categories is available on request from your school administrator or directly from our team.

08

Your compliance questions

Schools evaluating EduPilot for procurement or compliance review can request our security and data-handling documentation — including our Privacy Policy, Terms & Conditions, and this Data Compliance overview — as a combined package.

