Trust & Security

Your students' data, guarded like it's our own.

Vidyapeeth 360 holds some of the most sensitive records an institution can — children's data within the scope of India's Digital Personal Data Protection Act, 2023. The Act and 2025 Rules have staged commencement. This page explains, in plain language, how the platform protects it: how schools are isolated from each other, what our AI can and cannot see, how consent and retention work, and how money moves. It describes product controls, not legal certification. Forward it to your trust, your committee, or your IT reviewer.

- DPDP-supporting controls, not certification
- Configured AI identifier safeguards
- Deployment region reviewed before go-live

Last reviewed against the shipped product: August 2026.

Every school's data is walled off at the database layer

Each school on Vidyapeeth 360 is a separate tenant, and the separation is enforced by the database itself — PostgreSQL Row-Level Security — not just by application code. The database refuses to return a row that doesn't belong to the school making the request.

- **Fail-closed by design.** If a request ever arrives without a school context, it matches nothing — an empty result, never another school's data.
- **Two independent walls.** Application-level tenant filtering runs on top of the database-enforced isolation, so a bug in one layer is still caught by the other.
- **School groups are scoped too.** A group administrator for an education trust sees only their own group's member schools — never another group's.

AI with permission boundaries and configured privacy safeguards

Aira combines permission-scoped product tools, deterministic system evidence and optional model-written explanations. The prompt is never an access-control boundary,

and model-written text must be checked against the linked source record when the decision matters.

- **The default router pattern-redacts common identifiers.** Phone numbers, emails, Aadhaar, PAN and UPI IDs are detected by configured patterns. Names are tokenized only when the calling context supplies known values, so every AI call path still requires review.
- **System evidence stays authoritative.** Several assistants use deterministic reports or bounded numeric inputs. Model-written prose can still be wrong, so staff verify material figures and actions against the linked product record.
- **The verified student-AI health boundary is explicit.** Current student-AI context excludes the named health, infirmary, wellbeing and counselling sources. That is a verified boundary for those paths, not a blanket promise for every present or future integration.
- **Permissions remain the access boundary.** Assistant tools are expected to enforce tenant, role and record scope. A missing authorization check is treated as a security defect; a model instruction is never a substitute.

ONE CONFIGURED REDACTION PATH

YOUR ACCOUNTANT ASKS

“Has **Ananya Krishnan** (98400 12345) cleared the ₹18,500 term fee?”

THE AI PROVIDER RECEIVES

“Has [NAME_1] ([PHONE_1]) cleared the ₹18,500 term fee?”

The phone pattern is detected by default; the name token requires the calling flow to supply that known value. Example uses sample data.

Consent, retention, and breach-response evidence

Vidyapeeth 360 includes controls that can support a school's privacy programme as India's DPDP framework comes into force in stages. Product controls do not determine the school's lawful purpose, notice, consent validity, or legal retention period.

- **An append-only consent ledger.** Every consent grant, rejection, and withdrawal is a new immutable entry — database permissions prevent the application from editing or deleting past records. Withdrawing consent is as easy as granting it.
- **Classification-driven retention.** Short-lived data such as notifications, messages, and consent links can be purged past configured windows; protected record classes require a governed retention or erasure review.

- **An internal 72-hour evidence timer.** A recorded personal-data breach is tracked from open through notified to resolved. The school and its advisers still determine the legally required recipients, timing, content, and any extension.
- **Supported export and erasure paths.** An authorised export can be prepared for review, and erasure redacts eligible personal fields while records held by configured retention rules remain restricted.

Access control inside the school

Isolation between schools is only half the story — inside a school, staff see only what their role genuinely needs.

- **Two-step sign-in for staff, MFA enforced for admins.** Every staff login is password plus a one-time code, and multi-factor authentication is mandatory by policy for school and platform administrators.
- **Authenticator apps supported.** Staff can enrol an offline TOTP authenticator app, with single-use backup codes — no dependence on SMS delivery for the second factor.
- **Role-based permissions, resolved fresh on every request.** A revoked permission takes effect immediately — there is no stale session that keeps old access alive.
- **Teachers see their own classroom.** Record-level scoping limits a classroom teacher to the class-sections they actually teach; guardian contact details are masked outside them, and student medical records are restricted to the nurse and administrators.
- **Separation of duties on money.** Refunds, fee concessions, payroll, and payouts follow a maker-checker rule: the person who raises one can never approve their own.
- **An append-only audit trail.** Privileged actions land in a tamper-evident audit log retained for 7 years — the application has no ability to delete it.

School-controlled payment collection

Fee collection runs through the school's connected payment-gateway account. Vidyapeeth 360 records provider evidence against the invoice; the school reconciles settlement timing, deductions and final bank credit from provider or bank records.

- **Invoice-bound provider evidence.** A collection order and its verified callback remain tied to the invoice being paid.

- **A hash-chained payment audit log.** Every payment event is appended to a log where each entry cryptographically seals the one before it — a retroactive edit is mathematically detectable.
- **Paid means provider-confirmed.** An invoice is marked paid only on verified provider evidence — never because a checkout window closed. Final bank reconciliation remains with the school.
- **Exact to the paisa.** Money is stored as whole paise end-to-end, and receipts are numbered sequentially from an atomic counter — no rounding drift, no duplicate receipt numbers.
- **A production safety guard.** Outside of demo mode, the platform refuses to start with test-mode payment keys configured.

Operational security

The everyday disciplines behind everything above.

- **Secrets are encrypted.** Payment-gateway credentials and API secrets are encrypted at rest and managed through a cloud secrets manager — never stored in code.
- **Per-school webhook authentication.** Each school's inbound payment and messaging webhooks are verified with that school's own HMAC-signed token, so one school's token can never be used against another.
- **Backup controls reviewed before go-live.** Backup cadence, recovery objectives and restore testing are confirmed for your production deployment before launch.
- **Deployment region is reviewed before go-live.** Compute, database, storage and backup locations are deployment-specific and documented instead of being assumed from this website.

Who processes your data — and how to get our DPA

A school's deployment can involve the named service providers below, each limited to the role and data category shown. Which of them actually apply depends on what your school connects and enables — several are optional, and the payment gateway runs under the school's own provider agreement.

PAYMENT GATEWAY

Razorpay or Cashfree — the school's OWN connected account

Payer identity, invoice references and payment evidence, held under the school's direct gateway agreement.

WHATSAPP / SMS

MSG91, and Meta's WhatsApp Cloud API where a school configures it

Recipient phone numbers and school-approved template message content.

EMAIL DELIVERY

SendGrid, or the school's own SMTP service

Recipient email addresses and transactional message content.

VOICE AI (OPTIONAL)

Sarvam AI, for the vernacular speech features where enabled

Speech audio and its transcript for the requesting user's interaction, with identifier scrubbing applied to outbound text.

AI MODEL PROVIDER (OPTIONAL)

The model provider configured for enabled Aira flows

Identifier-redacted prompt text per the configured redaction path — the default router pattern-redacts common identifiers; name removal depends on the calling flow.

CLOUD INFRASTRUCTURE

Documented for each deployment before go-live (the reference architecture targets Amazon Web Services with CloudFront delivery)

Hosting of the school's workspace — compute, database, storage and backup locations are deployment-specific and documented, never assumed from this website.

WEBSITE ANALYTICS AND SESSION REPLAY

Google Analytics and Microsoft Clarity — this marketing site only, each loaded only with visitor consent and only where that provider is configured for the deployment

Anonymous marketing-site usage, and — for Clarity — anonymised interaction patterns such as clicks, scrolls and page structure. The school application itself is not in scope of this consent banner. Our analytics event contract excludes names, email addresses, phone numbers and student records.

Need it contractually? Request our Data Processing Agreement: legal@helprevx.com. The executed DPA and your written proposal govern the final provider list for your school's deployment.

Running the DPDP lens over this page? The DPDP guide for schools maps each privacy duty to its supporting control.

Questions — or something to report?

Running a security review for your committee? Email support@vidyapeeth360.com and we'll work through your questionnaire with you.

Need something to file? Download the trust pack (PDF · August 2026) — this page, verbatim, as of its review date (August 2026). The print button above always produces the current copy.

If you believe you've found a security vulnerability, email support@vidyapeeth360.com with “Security” in the subject line. We read, acknowledge, and investigate every good-faith report.

See also our Privacy Policy or contact us for anything else.