NewsLetter
April 2026

ALPHA MD®

From Awareness to Action:

Data Protection in Educational Institutions

No parent ever imagined that just filling an admission form in school will give them all required details made available before time for the best career counsellers and tutorials in the city.

Call this a luzury, overwhelming, privacy breach or information burn out, I would call this DPDPA violation.

How it all started ?

Educational institutions routinely collect a wide range of student data – from basic identifiers (names, student IDs, contact details) to academic records (grades, transcripts), health and disability information, family financial details, and even biometric and behavioral data.

These data are gathered via enrollment forms, school information systems, health and counseling records, digital learning platforms, attendance/bus trackers, and surveillance devices. In many countries, schools share or inadvertently expose rather sell this data to external “coaching” or tutoring services in shocking 10-15 Rs Per students (often through formal agreements, third-party vendors, exam-result disclosures, or ad hoc referrals)

Whats the unseen risk ?

1. The student and parent data are shared with coaching institutes without “Explicit consent” of the parent.
2. The method of collection is borne with many risks as proper safeguards and controls are not exercised during the collection and storage.
3. No formal agreement between educational institutions and coaching institutes.
4. Uncontrolled chain of sharing student’s names, pictures, grades and subjects marks on edtech apps, marketing agencies, data brokers, alumni networks.
5. Parent lose confidence and trust in the institution owing to negative publicity and complaints.

Some common student data leaks

2018 – India (Data Sale Websites): Medianama reported that over 50 websites (run by one person) were selling "expansive and exhaustive" databases on millions of Indian students. These leaked datasets covered engineering, medical, fashion and high-school students across multiple states.

2020-2021 – India (Exam Data Breaches): Security firms found student exam data being auctioned. CloudSEK revealed that data of hundreds of thousands of Common Aptitude Test (CAT) candidates was for sale on hacking forums. In 2021, India Today reported a website "studentdatabase.in" offering confidential information on millions of students

---

2023 (Jan) – India (Diksha App Exposure): A WIRED investigative report uncovered that India's DIKSHA education app (used by millions during COVID-19) had left a cloud server unprotected. This exposed 512 GB of data including: teachers' names, phone numbers, and emails (>1 million records), and students' full names, partially masked contact info, school enrollment and course progress for ~600,000 users.

2023 (Apr) – India (Bengaluru School Data Leak): Times of India reported that dozens of Bangalore parents received simultaneous calls and SMS from coaching institutes asking about their child's admissions, though the parents never contacted those institutes. Investigation revealed suspicion of a school data breach: parents' contact information (for both students and guardians) likely leaked from school records

Looking through DPDP lens

1. As per Chapter 2, section 4 of DPDP Act 2023, institutions must obtain explicit parental consent before sharing personal data
2. Retention time-period need to be defined by institutions during admission and parents must be informed 48 hrs prior to having any action related to erasure.
3. If event of any unauthorized sharing leading to data breach or detrimental effect on well being of the child, institution will be penalized up to ₹250 crore.
4. Institutions are compelled to immediately remove access of all child and parent data as soon as the consent is withdrawn.
5. Institution must inform immediately the parent about the occurrence of the data breach and to the Data protection board within 72 hrs of becoming aware of the same.

Mitigation Steps

Technical and organizational controls can greatly reduce these risks. Key recommendations in **Data Minimization:** Collect and retain only what is strictly necessary. For example, avoid collecting full Aadhaar/SSNs unless legally required; anonymize or truncate contact info when sharing. Delete outdated records (enrollment lists, alumni addresses) per strict retention policies.

Informed Consent and Transparency: Ensure students/parents know what data is collected and why. Obtain **explicit consent** for uses beyond core education (e.g. for sharing with external vendors or marketing). The DPDP Act emphasizes specific, informed consent. Provide clear opt-out options (e.g. for photo releases or surveys).

Encryption: Encrypt data at rest and in transit for all student data . This prevents simple data exfiltration. Use strong **cryptographic keys** and ensure secure storage of biometric templates (e.g. store only hashes of fingerprints).

Access Controls: Implement strict role-based access. Only authorized staff should view sensitive records. **Apply multi-factor authentication (MFA)** for admin portals. Maintain audit logs of who accessed what student data. The DOE guidance notes that improper disclosures of PII violate FERPA and advises logging all disclosures.

Data Protection Impact Assessments (DPIAs): Before rolling out new programs (e.g. using a new attendance app or data analytics tool), perform DPIAs **to identify privacy risks and mitigation.** This practice is required under GDPR for processing children's data, and recommended generally (India's DPDP Act and U.S. Student Privacy Pledge encourage similar reviews).

Anonymization/Pseudonymization: Where possible, use de-identified data. For research or statistics, scrub direct identifiers and use codes. However, follow caution that **"anonymized" student data must be genuinely de-identified** (hard to re-link. For example, share aggregated performance data with third parties rather than individual transcripts.

Secure Third-Party/Vendor Management: Vet any external **education vendors** rigorously. Contracts should forbid unauthorized data sharing or marketing. Require vendors to follow data protection laws and conduct security audits. For instance, if a school app developer warns it may share data, renegotiate or find an alternative. The Bangalore case highlighted risks when schools had contracts with vendors but lacked oversight.

Encryption and Safe Storage of Biometric Data: If biometrics are used (e.g. fingerprint scanners for lunch), store templates locally or in a secure enclave, not on a publicly reachable server. **Do not transmit raw biometric images.** Regularly clear logs.

Training and Awareness: Regularly train staff and students on data security. Phishing and weak passwords are common causes of breaches; training can reduce these risks. The ICO and privacy advocates stress that **"security protections"** must include mandatory training for all who handle student data. Culture change is vital: if teachers understand the danger of, say, emailing gradebooks insecurely or posting exam results online, accidental leaks become less likely.

For Parents and Students

Be Informed: Parents should ask schools to disclose what data they collect and with whom it is shared. They can review privacy policies or submit subject-access requests under applicable laws (DPDP)

Consent and Opt-Out: Exercise opt-out rights (e.g. decline publication of photos, refuse surveys) where available. Carefully read consent forms before allowing any personal data to go to third parties. Parents may refuse non-essential data sharing with vendors (India's DPDP requires explicit consent for child data beyond core education).

Monitor Accounts: Since children's data can be used fraudulently, parents should regularly check children's credit reports once they turn 18, and consider credit freezes when necessary.

Report Violations: If parents see suspicious calls or ads implying a data leak (as in the Bangalore case), they should alert the school administration and, if needed, data protection authorities.

Privacy Education: Teach students basic digital hygiene: strong passwords on school accounts, caution with third-party apps, and to report any cyberbullying or phishing attempts tied to school data.

Strategic Support for Stronger Data Processor Oversight & End-to-End DPDPA Compliance

At Alpha MD, we help educational institutions build, assess and sustain accountability across the privacy chain. Our services include:

- Develop and review contracts to identify privacy gaps in vendor relationships.
- Assist in developing and validating privacy notices in line with DPDP Act.
- End to end compliance and gap analysis of digital products and third party integrations.
- Develop consent management framework for personal data processing.

If you are new to DPDP Act language or need to understand how to start your compliance journey, feel free to reach out to us for queries and DPDP implementation support.

FOLLOW US ON SOCIAL MEDIA

+91 97697 96321 info@alphamd.com www.alphamd.com