Education & EdTech

DPDPA 2023 Implementation Handbook

Digital Personal Data Protection Act, 2023 • India

For schools, universities, coaching institutes, online learning platforms, and exam proctoring services.

1. Overview & Applicability

Education institutions and EdTech platforms process the personal data of children — the most protected category under the DPDPA. The Act requires verifiable parental consent before processing any data of individuals under 18. Behavioural tracking, profiling, and targeted advertising to children is explicitly prohibited. Schools, universities, and learning platforms must overhaul their data practices, particularly their use of third-party analytics, proctoring tools, and learning management systems.

2. Key Definitions Under DPDPA

These definitions govern how the Act applies to your sector:

Child	Any individual below 18 years of age — attracts the highest level of DPDPA protection.
Verifiable Parental Consent	Consent from a parent or guardian for processing a child's data — must be verifiable, not just a checkbox.
Student Data	Names, roll numbers, academic records, performance data, health records, biometrics, and learning behaviour — all personal data.
Behavioural Tracking	Tracking a child's online activity, learning patterns, or content consumption for profiling — prohibited without consent.
Data Processor	LMS vendors (Moodle, Canvas), proctoring platforms, ERP systems, cloud storage — all require DPAs.
Purpose Limitation	Student performance data cannot be shared with employers or used for marketing without separate consent.

3. Core Compliance Obligations

Every entity in this sector that processes personal data must comply with the following obligations:

1. **Parental Consent System**
   Implement a verifiable parental consent mechanism for all students under 18. Physical consent forms or digital verification with parent's identity validation.
2. **No Profiling of Children**
   Completely prohibit behavioural tracking, interest profiling, or targeted advertising on any platform accessible to children.
3. **Third-Party EdTech Tools**
   Audit all third-party tools used in the classroom — Google Classroom, Zoom, proctoring software. Ensure each has a DPA and complies with DPDPA.
4. **Exam Proctoring**
   Biometric and facial recognition data used in remote proctoring is sensitive. Disclose to students and parents; obtain consent; delete after exam cycle.
5. **Alumni Data**
   Maintain a separate consent process for alumni — do not use student data for alumni communications without consent.
6. **Research & Publication**
   Academic research using student data requires anonymisation and separate ethics/consent approval.

7	**Student Rights** Allow students (and parents for minors) to access, correct, and request deletion of academic records.
8	**Grievance Mechanism** Appoint a Grievance Officer. For schools, the Principal can be the designated officer with a clear escalation path.

4. Implementation Checklist

Use this checklist to track your DPDPA compliance readiness:

- ☐ Audit all digital platforms used in your institution — LMS, ERP, attendance apps, proctoring tools.
- ☐ Implement verifiable parental consent for all students under 18 before using any digital platform.
- ☐ Disable all behavioural tracking, interest-based advertising, and profiling on student-facing platforms.
- ☐ Execute Data Processing Agreements with all EdTech vendors, cloud providers, and SaaS tools.
- ☐ Update your institution's privacy policy — publish it on your website and share with parents at admission.
- ☐ Build a process for parents/students to access, correct, or erase academic data.
- ☐ Appoint a Grievance Officer and communicate contact details to students and parents.
- ☐ Review retention schedules — how long do you keep academic records, attendance data, and exam scripts?
- ☐ Train teachers, administrators, and IT staff on student data privacy obligations.
- ☐ Audit all exam proctoring data — biometric and video data must be deleted after the exam cycle.
- ☐ Do not share student data with third parties (employers, advertisers) without explicit consent.
- ☐ Review your scholarship and fee-waiver application processes — sensitive financial data collected here.

5. Applicable Penalties

The Data Protection Board of India (DPBI) may impose the following penalties for non-compliance:

Rs. 250 Crore	Failure to implement reasonable security safeguards resulting in a personal data breach
Rs. 200 Crore	Breach of obligations related to processing children's personal data
Rs. 150 Crore	Failure to fulfill obligations as a Significant Data Fiduciary (SDF)
Rs. 50 Crore	Failure to comply with Data Principal rights or other provisions of the Act

6. Implementation Roadmap

Follow this phased approach to achieve full DPDPA compliance:

1	**Month 1: Platform Audit** List all digital tools and platforms used. Identify which collect student data and which serve children.
2	**Month 2: Parental Consent Design** Design and implement verifiable parental consent forms for each platform used with minors.
3	**Month 3: Vendor DPAs** Contact all EdTech vendors and execute DPAs. Remove or replace non-compliant vendors.
4	**Month 4: Policy Update** Update privacy policy, student handbook, and admission forms to reflect DPDPA obligations.
5	**Month 5: Rights & Grievance** Build student/parent rights request process. Appoint and train Grievance Officer.
6	**Month 6+: Annual Review** Annual audit of all third-party tools, student data stores, and consent records.

👶 Priority: Children's data is the most protected category. Processing children's data without verifiable parental consent carries a penalty of up to Rs. 200 Crore. Act immediately.