



Importance of Digital Personal Data Protection (DPDP) Act, 2023 for Educational Institutions: A Comprehensive Review

Dr. Pawan Kumar

Chancellor, Mahatma Gandhi University, Sikkim

Abstract: *Background: Educational institutions are among the largest processors of personal data including minors' data. With rapid digitization of admission, Learning Management Systems (LMS), fee payments and surveillance, data vulnerability has increased. Objective: This review article analyzes the provisions of the Digital Personal Data Protection Act, 2023 and its relevance, mandatory requirements, and implementation challenges for schools, colleges and universities in India. Methods: A doctrinal and systematic review of the DPDP Act, 2023, Draft DPDP Rules 2025, Data Protection Board notifications, and secondary literature from 2018-2026 was conducted. Comparative analysis with GDPR, FERPA and Indian IT Act was performed. Results: The Act imposes fiduciary obligations on educational institutions including verifiable parental consent under Section 9, purpose limitation, data minimization, breach notification within 72 hours, and penalties up to INR 250 crore. Conclusion: DPDP compliance is not merely legal obligation but strategic enabler of trust, data security and global academic collaboration. A phased implementation model is proposed.*

Keywords: DPDP Act 2023; Data Fiduciary; Student Privacy; Children Data; Educational Institutions; Data Protection Board of India; Verifiable Parental Consent.

1. Introduction: The digitization of education accelerated by NEP 2020 and COVID-19 has led to creation of vast digital footprints of students. According to Ministry of Education, over 300 million students' data is processed through UDISE+, DIKSHA, APAAR and institutional ERPs. Previously, data protection in India was governed by Information Technology Act, 2000 and SPDI Rules 2011, which lacked comprehensive framework, regulatory authority and stringent penalties (maximum INR 5 crore). The Justice B.N. Srikrishna Committee (2018), JPC Report (2021) and Supreme Court judgment in K.S. Puttaswamy v. Union of India (2017) recognizing privacy as fundamental right paved way for DPDP Act, 2023, enacted on 11th August 2023. Educational institutions qualify as Data Fiduciaries under Section 2(i) as they determine purpose and means of processing. Given that 60-70% of school population is under 18 years, Section 9 (Children's Data) makes compliance critical.

2. Research Methodology

2.1 Research Design: Doctrinal legal research with systematic literature review.

2.2 Data Sources: Primary: DPDP Act 2023 bare act, Draft DPDP Rules 2025, MeitY notifications. Secondary: 40 peer-reviewed articles, government reports, legal commentaries indexed in Scopus, Hein Online, Manupatra (2018-2026).

2.3 Inclusion Criteria: Articles focusing on DPDP Act, educational data privacy, children privacy, GDPR in education.

2.4 Analysis Framework: Thematic analysis using fiduciary obligations, rights of Data Principals, and implementation challenges as themes.

3. Research Gap: Existing literature predominantly focuses on DPDP Act from corporate and IT industry perspective. Limited empirical studies address:

- (a) Applicability to schools and higher education institutions as fiduciaries,
- (b) Operationalization of verifiable parental consent in Indian school context,
- (c) Cost of compliance for budget private schools,
- (d) Intersection with existing education laws (RTE Act, UGC regulations on student records). This review bridges that gap.

4. Overview of DPDP Act, 2023 - Key Provisions: The Act consists of 9 Chapters, 44 Sections and a Schedule on penalties. It applies to digital personal data processed within India, and outside India if in connection with offering goods/services to Data Principals in India. Core architecture:

- Data Principal (Sec 2(j)): Student, parent, teacher, staff.
- Data Fiduciary (Sec 2(i)): Educational Institution.
- Data Processor (Sec 2(k)): Third-party vendor processing on behalf of fiduciary (e.g., Fedena, Moodle, fee gateway).
- Data Protection Board of India (Sec 18-22): Adjudicatory body with digital office.
- Consent Manager (Sec 2(f)): Platform to manage consent.

Seven Principles: Lawfulness, Purpose Limitation, Data Minimization, Accuracy, Storage Limitation, Reasonable Security Safeguards, Accountability.

5. Student Data Ecosystem in Educational Institutions: Educational institutions collect diverse categories of personal data:

Category	Examples	Sensitivity	Typical Storage
Identity Data	Name, DOB, Aadhaar No., Photo, Biometric attendance	High	ERP, Admission Form
Academic Data	Report cards, Learning analytics, Disciplinary records	Medium	LMS, UDISE+
Health Data	Medical certificate, Disability, Mental health counselling	High	Infirmiry records
Financial Data	Bank account for scholarship, Fee payment details	High	Fee gateway, ERP

Location & Surveillance	GPS bus tracking, RFID ID card, CCTV	High	Transport app, Security server
Behavioural Data	Online class engagement, Library logs, Internet usage	Medium-High	LMS logs

Table 1: Taxonomy of Student Personal Data Processed by Educational Institutions

6. Special Protection For Children's Data - Section 9: Section 9 is the cornerstone for schools.

6.1 Verifiable Parental Consent: Processing of personal data of a child (<18 years) or person with disability with lawful guardian is permissible ONLY with verifiable consent of parent/guardian. Draft Rules 2025 propose verification via:

- (a) tokenized identity through DigiLocker,
- (b) virtual token mapped to parent's government ID,
- (c) existing consent management system of school with due diligence.

6.2 Prohibitions: Section 9(3) prohibits:

(i) processing likely to cause detrimental effect on well-being of child, (ii) tracking or behavioural monitoring of children, (iii) targeted advertising directed at children. This impacts EdTech advertising inside school apps and use of cookies for profiling.

6.3 Comparison with Global Norms: Similar to GDPR-K (Art 8) requiring 13-16 years age threshold and US COPPA (13 years), but DPDP sets 18 years, making Indian law stricter. Unlike FERPA which allows school official exception, DPDP requires explicit consent.

6.4 Practical Challenges: Verification of guardianship in divorced parents, orphan students, low digital literacy of parents, fake consent.

7. What is Mandatory for Educational Institutions?

- 7.1 Privacy Notice (Sec 6): Notice in English + 22 scheduled languages, containing: data collected, purpose, retention, grievance officer details, rights of Data Principal.
- 7.2 Consent Architecture: Freely given, specific, informed, unconditional, unambiguous with clear affirmative action. Bundled consent for admission + marketing is invalid.
- 7.3 Appointment of DPO and Grievance Officer: Publish contact on website, notice board, prospectus. Response to grievance within 7 days.
- 7.4 Data Security (Sec 8(4)): Reasonable security safeguards including encryption, pseudonymization, access control, logging, backup.
- 7.5 Breach Notification (Sec 8(6)): Notify Board and affected Data Principals within 72 hours of becoming aware, as per Draft Rules 2025.
- 7.6 Retention and Erasure (Sec 8(7)): Delete data when purpose fulfilled or consent withdrawn, unless retention mandated by law (e.g., UGC mandates 5-year retention of degrees).
- 7.7 Vendor Management (Sec 8(2)): Data fiduciary liable for processor's actions. Data Processing Agreement mandatory.

7.8 Data Protection Impact Assessment: Recommended for large universities, especially when deploying AI-based proctoring or facial recognition.

8. Parental Role And Rights Of Data Principal: Parents act as authorized representatives under Sec 9. Their rights:

- Right to Information (Sec 11): Summary of data processed, processing activities, identities of processors.
- Right to Correction and Erasure (Sec 12): Correct inaccurate, update obsolete data.
- Right to Grievance Redressal (Sec 13): Approach Board if not satisfied.
- Right to Nominate (Sec 14): Nominate person to exercise rights in case of death/incapacity of Data Principal.

Duties of Data Principal (Sec 15): Not to impersonate, not to provide false information, not to file false complaints.

Parent-School Collaboration Model: Schools should conduct DPDP literacy during PTMs, provide consent dashboards.

9. Implementation Roadmap - Flowchart Description: Proposed 6-Phase Model:

Phase 1 - Discovery & Audit (Week 1-2): Data mapping, Record of Processing Activities (RoPA), identify Significant Data Fiduciary status.

Phase 2 - Gap Analysis & Policy Drafting (Week 3-5): Privacy policy, retention schedule, breach playbook, children data policy.

Phase 3 - Legal & Governance (Week 6): Appoint DPO, Grievance Officer, Data Protection Committee.

Phase 4 - Technical Controls (Week 7-10): Implement encryption, access control matrix, consent manager, auto-deletion scripts, CCTV notice.

Phase 5 - Third-Party Alignment (Week 11-12): Renegotiate contracts with ERP/LMS vendors, cloud storage localization check.

Phase 6 - Training & Audit (Ongoing): Teacher training, student digital citizenship curriculum, annual internal audit.

Figure 1: DPDP Implementation Flowchart - Start -> Data Inventory -> Risk Classification -> Policy Creation -> DPO Appointment -> Technical Safeguards -> Parental Consent System -> Vendor Compliance -> Training -> Continuous Monitoring -> End.

10. Penalties And Enforcement

Board may impose graded penalties after inquiry, considering nature, gravity, duration, mitigation efforts.

Violation Type	Relevant Section	Maximum Fine	Example in Education
Failure to implement security safeguards	Sec 8(4)	INR 250 Crore	Ransomware leak of student Aadhaar database

Failure to notify breach	Sec 8(6)	INR 200 Crore	Not informing parents after fee portal breach
Violation of children's obligations	Sec 9	INR 200 Crore	Tracking children via ed-tech ads without parental consent
Non-compliance with Data Principal rights	Sec 11-13	INR 50 Crore	Not providing data copy when parent requests
Breach of additional obligations of SDF	Sec 10	INR 150 Crore	Large university not appointing DPO/auditor
Other non-compliances	General	INR 50 Crore	No grievance officer, invalid consent

Table 2: Penalty Schedule under DPDP Act, 2023 (Schedule)

11. Institutional Compliance Checklist

Domain	Check Item	Status	Evidence
Governance	DPO & Grievance Officer appointed & published	☐ Yes ☐ No	Website link, Notice board photo
Notice	Privacy notice in English + Hindi + local language	☐ Yes ☐ No	Admission form copy
Consent	Separate consent for child data, verifiable parental consent	☐ Yes ☐ No	Consent logs
Data Minimization	Only last 4 digits of Aadhaar collected	☐ Yes ☐ No	Form audit
Security	Encryption at rest & in transit, RBAC implemented	☐ Yes ☐ No	IT audit report
Retention	Retention schedule defined & auto-deletion enabled	☐ Yes ☐ No	Policy document
Breach	Breach response plan, 72-hr notification SOP	☐ Yes ☐ No	SOP document
Vendors	DPA signed with all processors, data localization verified	☐ Yes ☐ No	Agreements
Training	Annual DPDP training for staff & students	☐ Yes ☐ No	Training attendance
Rights	Mechanism for access/correction/erasure requests	☐ Yes ☐ No	Grievance register

Table 3: DPDP Compliance Checklist for Educational Institutions

12. Benefits And Challenges

Benefits: Enhanced parental trust, reduced litigation, alignment with NEP 2020 digital initiatives, improved eligibility for international collaborations (GDPR adequacy), reduction in data storage cost, prevention of identity theft and cyberbullying.

Challenges: Cost for budget private schools, low digital literacy of parents for consent verification, lack of skilled DPOs in education sector, conflict with mandatory reporting under POCSO/RTE vs erasure requests, legacy systems not designed for consent granularity.

13. Recommendations

1. For Policy Makers: Issue sector-specific guidelines for education (similar to UK ICO's Education guidance), create model privacy notices for schools.
2. For Institutions: Adopt Privacy by Design in ERP procurement, create consent dashboard for parents, implement APAAR ID with privacy considerations.
3. For EdTech Vendors: Achieve ISO 27001, SOC 2, ensure data localization, provide deletion APIs.
4. For Parents: Participate in consent literacy, exercise rights responsibly.
5. Future Research: Empirical study on compliance cost, effectiveness of verifiable parental consent models in rural India, AI proctoring and DPDP intersection.

14. Conclusion: The DPDP Act, 2023 marks paradigm shift from institution-centric data ownership to principal-centric data custodianship. For educational institutions, which are custodians of future citizens' data, compliance is both legal mandate and ethical responsibility. Early adoption of privacy-by-design, robust parental consent mechanism and strong security safeguards will differentiate institutions as trustworthy. The proposed phased model and checklist provide practical starting point. Further longitudinal research is needed to assess implementation effectiveness.

15. References

- Almeida C, et al. Comparative analysis of FERPA, GDPR and DPDP in school context. *Educ Law J.* 2023;24(4):401-423.
- Banerjee S, Gupta R. Cost of compliance with DPDP Act for SMEs and educational institutions. *Econ Polit Wkly.* 2024;59(42):33-40.
- Bhatt P, Singh R. Data privacy in Indian higher education: challenges of DPDP Act. *J Educ Technol.* 2024;15(2):45-58.
- Burman A, Rai S. India's Data Protection Law: Comparison with GDPR. *Vidhi Centre for Legal Policy;* 2023.
- Central Board of Secondary Education. Guidelines on handling student data and UDISE reporting. *CBSE Circular;* 2024.
- Chaudhary S. Enforcement by Data Protection Board of India: penalty jurisprudence. *Indian J Data Prot.* 2025;1(1):5-27.

- Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506. Federal Trade Commission; 1998.
- Data Security Council of India. State of Data Privacy in Education Sector. DSCI Report; 2024.
- Davis FD. Perceived usefulness, ease of use and user acceptance of information technology. MIS Q. 1989;13(3):319-340.
- European Parliament. General Data Protection Regulation (EU) 2016/679. Official Journal of European Union. 2016.
- Government of India. National Education Policy 2020. Ministry of Education; 2020.
- Greenleaf G. Global Data Privacy Laws 2024: 162 National Laws. Privacy Laws Business Int Rep. 2024; 182:1-19.
- Information Commissioner's Office (UK). Data protection in schools toolkit. ICO; 2023.
- Justice B N Srikrishna Committee. A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians. Report. 2018.
- Kulkarni A, Patel M. EdTech and children's data: risk of behavioural profiling. Child Rights Law Rev. 2024;12(2):88-105.
- Kumar A, Jain P. Privacy by design in Learning Management Systems: aligning Moodle with DPDP. Educ Inf Technol. 2024;29:15233-15255.
- Mathews S, Srivastava A. Verifiable parental consent: technical models for India. Int J Cyber Law. 2025;3(1):22-38.
- Mehta R. Role of Data Protection Officer in universities. Univ News. 2024;62(15):12-18.
- MeitY. Advisory on data localisation and cross-border transfer under DPDP. 2025.
- Ministry of Education. Unified District Information System for Education Plus (UDISE+) 2023-24. New Delhi: MoE; 2024.
- Ministry of Electronics and Information Technology. Draft Digital Personal Data Protection Rules, 2025. MeitY; 2025 Jan 3.
- Ministry of Law and Justice. The Digital Personal Data Protection Act, 2023. The Gazette of India. 2023 Aug 11.
- Nair D, et al. Data breach incidents in Indian educational institutions: systematic review 2019-2024. Comput Secur J. 2025;142:103856.
- National Institute of Educational Planning and Administration. APAAR and Data Privacy: Issues and Safeguards. NIEPA Policy Brief; 2024.
- Nissenbaum H. Privacy in Context: Technology, Policy, and Integrity of Social Life. Stanford: Stanford Univ Press; 2010.
- Organisation for Economic Co-operation and Development. OECD Recommendation on Children in Digital Environment. OECD; 2021.

- Raghunathan A. Accountability and Data Fiduciary obligations under Section 8: implications for schools. J Indian Law Inst. 2024;66(3):289-310.
- Sharma L, et al. Awareness of DPDP Act among school teachers in Delhi NCR: a cross-sectional study. Indian J Educ Res. 2025;9(1):54-67.
- Singh K, et al. Biometric attendance and student privacy: a legal-technical audit. Int J Educ Manag. 2024;38(5):1121-1138.
- Solove DJ. Understanding Privacy. Cambridge: Harvard University Press; 2008.
- Sreenivasulu NS, Sharma V. Children's data protection under DPDP Act 2023: a critical analysis. Indian J Law Technol. 2024;20(1):112-134.
- Supreme Court of India. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
- U.S. Department of Education. Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g. 1974.
- University Grants Commission. Regulations on maintenance of student records and data security. UGC; 2023.
- WhatsApp LLC v. Union of India. Intermediary guidelines and data protection: Delhi High Court observations. 2024.
- World Economic Forum. Data Protection in Education 4.0: Global Toolkit. WEF; 2023.

Citation: Kumar. P., (2026) “Importance of Digital Personal Data Protection (DPDP) Act, 2023 for Educational Institutions: A Comprehensive Review”, *Bharati International Journal of Multidisciplinary Research & Development (BIJMRD)*, Vol-4, Issue-08, August-2026.