



Importance of the Digital Personal Data Protection (DPDP) Act, 2023 for Educational Institutes in India

Miss Adersikha Pradhan

LLB Student, Mahatma Gandhi University, Sikkim

Abstract: *Digital transformation has made educational institutions intensive users and custodians of personal data. Admissions, student information systems, attendance, examinations, fee administration, scholarships, learning-management systems, digital classrooms, identity verification, placement services, CCTV and other institutional processes may involve personal information relating to students, parents, faculty and staff. The Digital Personal Data Protection Act, 2023 (DPDP Act) establishes a legal framework for processing digital personal data in India, while the Digital Personal Data Protection Rules, 2025 provide operational detail and a phased commencement framework.[1,2] The education sector requires particular attention because institutions may process data relating to children, and Section 9 of the Act establishes additional requirements for children's personal data.[1] This review examines the relevance of the DPDP framework to educational institutes, focusing on student privacy, children's data, parental or lawful-guardian roles, transparency, consent, security safeguards, data retention, grievance redressal, breach management, third-party service providers and penalties. It proposes a practical institutional implementation model based on data inventory, purpose mapping, governance, privacy notices, access control, vendor management, retention schedules, incident response and periodic review. The article also discusses the phased commencement of the Act and Rules and highlights the need for institutions to distinguish statutory requirements that are currently in force from provisions scheduled to commence later. The paper concludes that data protection should be treated as an institution-wide governance responsibility rather than solely an information-technology function.*

Keywords: *Digital Personal Data Protection Act; DPDP Rules 2025; Educational Institutions; Student Privacy; Children's Data; Parental Consent; Data Governance; Cyber security; Personal Data; India.*

1. Introduction: Education has become increasingly dependent on digital systems. A contemporary school, college or university may collect and process information from the point of admission through graduation and alumni engagement. Student information may move between admission portals, student information systems, examination systems, finance offices, learning-management systems, cloud platforms, payment gateways, communication services and external technology providers. The growth of technology therefore creates both educational opportunities and new responsibilities concerning privacy, security and responsible data governance.[3-7]

The DPDP Act, 2023 was enacted on 11 August 2023. Its stated objective is to provide for processing of digital personal data in a manner that recognises individuals' right to protect their personal data while also recognising the need to process personal data for lawful purposes.[1] The Act defines a child as an individual

who has not completed eighteen years of age and places additional obligations on Data Fiduciaries when processing children's personal data.[1]

For educational institutions, the legal question is not simply whether data are collected electronically. The more important governance questions are: What personal data are collected? For what purpose? Who can access them? How long are they retained? Which external providers receive them? What safeguards are in place? What happens when a data breach occurs? How can a Data Principal exercise applicable rights? These questions form the basis of a practical institutional data-protection programme.

2. Objectives of the Review

- To explain the relevance of the DPDP Act, 2023 to educational institutions in India.
- To identify major categories of student and institutional personal data.
- To examine the additional legal considerations relating to children's personal data.
- To analyse institutional responsibilities concerning notice, consent, security, retention and grievance redressal.
- To examine the statutory penalty framework and its implications for institutional risk management.
- To develop a practical DPDP implementation framework for educational institutions.
- To identify research and policy gaps concerning learner-data governance in India.

3. Methodology: This article adopts a doctrinal and narrative review methodology. Primary legal materials were prioritised, including the Digital Personal Data Protection Act, 2023, official commencement notification, Digital Personal Data Protection Rules, 2025, and official materials issued by the Ministry of Electronics and Information Technology (MeitY). Secondary materials were consulted to understand the education-sector context, including UNICEF guidance on children's data and schools, UNESCO material on technology in education, and recent Indian policy analysis on learner-data governance.[1-15]

The review is primarily qualitative. Statutory provisions were organised into thematic areas relevant to educational institutions: data governance, student privacy, children's data, consent and notice, security, breach response, rights and grievance redressal, vendors, retention and penalties. The proposed implementation framework is an academic model and should be adapted to the institution's size, governance structure, processing activities and applicable sectoral requirements.

4. Digital Personal Data Protection Act, 2023: Overview: The DPDP Act establishes the concepts of Data Principal, Data Fiduciary, Data Processor, Consent Manager, child and Data Protection Board. A Data Fiduciary is the person who alone or jointly determines the purpose and means of processing personal data. In an educational setting, an institution may function as a Data Fiduciary where it determines why and how student or staff personal data are processed. External technology providers may process information on the institution's behalf and may therefore have a different role under the Act.[1]

The Act is not limited to cybersecurity. It combines rights of Data Principals with duties of Data Fiduciaries. Relevant institutional themes include lawful processing, notice, consent where applicable, security safeguards, breach-related obligations, grievance redressal, children's data, and additional obligations that may apply if an institution is notified as a Significant Data Fiduciary.[1]

5. Key Legal Terms for Educational Institutions

Term	Meaning / educational example
Data Principal	The individual to whom personal data relates; for a child, the statutory definition includes the parent or lawful guardian.[1]
Data Fiduciary	Entity deciding the purpose and means of processing; an institution may occupy this role for its own student administration.[1]
Data Processor	Entity processing personal data on behalf of a Data Fiduciary; examples can include certain technology vendors.[1]
Child	An individual who has not completed 18 years under the Act.[1]
Consent Manager	Registered entity enabling Data Principals to give, manage, review and withdraw consent through an accessible platform.[1,2]
Personal Data	Data about an individual who is identifiable by or in relation to that data.[1]
Processing	Digital operations performed on personal data, within the scope of the Act.[1]

6. Student Data in the Educational Ecosystem: Educational institutions should first understand their data landscape. A data inventory is the foundation for meaningful compliance because an institution cannot protect information effectively if it does not know what information it holds, where it is stored, who uses it, or with whom it is shared.

Data category	Examples	Institutional risk / control
Identity	Name, date of birth, photograph, student ID	Role-based access; avoid unnecessary public disclosure
Contact	Mobile number, email, address	Limit access; use official channels
Academic	Marks, grades, attendance, assignments	Restricted academic access; confidentiality
Financial	Fee records, scholarship information	Finance-only or need-to-know access
Identification	Identity documents and verification information	Secure storage; limited access
Health/welfare	Medical or disability-related information where collected	Strong confidentiality; purpose-specific use
Biometric	Fingerprint, face or other biometric information where lawfully used	High security; documented purpose and access
Digital learning	LMS activity, submissions, assessment data	Purpose limitation; vendor controls

CCTV/security	Images and recordings	Defined access and retention period
Parent/guardian	Contact and verification information	Restricted access; accuracy controls

7. Importance of Student Privacy: Student privacy is closely connected with dignity, safety, trust and responsible institutional governance. UNICEF notes that educational technologies can produce substantial benefits while also creating privacy, security and governance risks when children's data are collected and used by schools, governments, third parties and commercial actors.[5-7] In India, recent analysis has similarly identified learner-data governance as an emerging policy issue in digital education.[8]

Student privacy does not mean that an institution cannot maintain academic records. Rather, privacy governance requires institutions to establish appropriate purposes, access controls, safeguards, transparency and retention practices. Academic administration and privacy protection can therefore operate together through responsible data governance.

8. Children's Personal Data: Children receive heightened protection under the DPDP Act. Section 9 applies specific requirements to the processing of children's personal data. The Act requires verifiable consent of the parent or lawful guardian before processing a child's personal data, in the prescribed manner. It also restricts processing that is likely to cause detrimental effects on the well-being of a child and addresses tracking, behavioural monitoring and targeted advertising directed at children, subject to statutory provisions and applicable exceptions.[1]

The 2025 Rules specify mechanisms relevant to verifiable consent and provide further detail for processing involving children. Educational institutions should therefore maintain a separate child-data procedure rather than relying only on a general adult privacy notice.[2]

Institutional control	Recommended practice
Age determination	Establish a documented process for identifying whether the child provisions apply.
Parent/guardian verification	Use the prescribed verification mechanism where required.
Purpose limitation	Document the educational or administrative purpose for each processing activity.
Monitoring	Review whether any digital tool performs tracking or behavioural monitoring involving children.
Advertising	Ensure institutional practices do not facilitate prohibited targeted advertising directed at children.
Vendor controls	Contractually and technically control child-data processing by external platforms.
Deletion/retention	Review whether continued retention remains necessary or legally required.

9. Role of Parents and Lawful Guardians: Parents and lawful guardians can support children's privacy by reviewing institutional notices, understanding the purposes for which information is collected, using official communication channels and raising concerns about inappropriate disclosure. Where the law requires verifiable parental consent, institutions should use a reliable process rather than treating a general admission declaration as automatically sufficient for every subsequent processing activity.[1,2]

At the same time, parental consent should not be treated as unlimited permission. Institutional governance should continue to address purpose, security, access, retention, vendor management and other applicable requirements.

10. Notice and Transparency: The DPDP Rules, 2025 require a notice to be presented in a manner understandable independently of other information and to provide, in clear and plain language, an itemised description of personal data and the specified purpose or purposes of processing. The Rules also address communication links and mechanisms through which Data Principals can access relevant functions, including withdrawal of consent where applicable.[2]

For universities, a privacy notice can be organised around four questions:

- What personal data are we collecting?
- Why are we collecting and using it?
- Which departments or service providers may receive it?
- How can the Data Principal exercise applicable rights or raise a complaint?

11. Consent and Lawful Institutional Processing

Consent is an important element of the DPDP framework, but educational institutions should not design compliance around the assumption that every administrative activity is identical. The Act recognises certain legitimate uses and other lawful grounds, while consent has specific statutory requirements.[1] Institutions should therefore map each processing activity to the applicable legal basis or permitted ground and avoid collecting broad consent merely as a substitute for governance.

Processing activity	Questions for institutional review
Admission	What information is required and for which purpose?
Attendance	Is the data necessary for attendance administration? Who needs access?
Examination	Which records must be retained for academic/regulatory purposes?
Fees	Which payment and financial information is processed and by whom?
Scholarships	Which information is required to administer the scheme?
LMS	What learner activity is collected by the platform?
CCTV	What is the purpose and defined retention period?
Biometrics	Is the system necessary, appropriately governed and securely implemented?
Research	Is the dataset identifiable, anonymised or otherwise governed under the applicable framework?

12. Data Minimisation and Purpose Specification: A practical institutional test is: “Do we need this information for the stated purpose?” Data fields that do not have a clear purpose should be reviewed. Minimisation can reduce the consequences of a breach, simplify access control and reduce unnecessary administrative exposure.

A data inventory should record at least:

- Data field or category
- Purpose of processing
- Source of the data
- Department responsible
- Systems in which it is stored
- External recipients or processors
- Retention requirement
- Access roles
- Security controls
- Deletion or archival mechanism

13. Data Security: The Act places an obligation on Data Fiduciaries to take reasonable security safeguards to prevent personal-data breaches. The Schedule provides a maximum penalty of ₹250 crore for failure to take reasonable security safeguards.[1] The monetary ceiling demonstrates why information security should be integrated into institutional governance rather than left solely to informal IT practices.

Control area	Examples
Identity and access	Unique accounts, strong authentication, role-based access
Endpoint security	Updates, malware protection, device controls
Network security	Firewalls, segmentation, secure remote access
Database security	Encryption, restricted administrator access, logging
Backups	Regular tested backups and recovery procedures
Monitoring	Security logs, alerts and periodic review
Staff awareness	Phishing awareness, password hygiene, reporting procedures
Vendor security	Due diligence and contractual security requirements
Incident response	Documented detection, containment, assessment and notification workflow

14. Role-Based Access Control: A core principle for educational institutions is that access should correspond to institutional responsibility. A faculty member may require attendance and academic

information but should not automatically have access to finance or unrelated student records. Similarly, finance staff may need fee information but not detailed counselling records. Role-based access reduces accidental disclosure and limits the consequences of compromised accounts.

15. Faculty and Staff Responsibilities

- Use only authorised institutional systems for institutional records.
- Do not share passwords or authentication tokens.
- Do not publish student personal information unnecessarily on public websites or social media.
- Verify recipients before sending student records.
- Store downloaded records only when necessary and securely.
- Report suspected loss, unauthorised access or mistaken disclosure promptly.
- Complete periodic privacy and cybersecurity awareness training.
- Follow the institution's retention and deletion procedures.

16. Third-Party Vendors and Data Processors: Educational institutions increasingly rely on ERP systems, learning-management systems, online examination platforms, cloud storage, payment services, communication tools, biometric systems and other vendors. Vendor selection should therefore include a data-protection review rather than focusing only on price and functionality.

Vendor due-diligence question	Evidence to seek
What data are processed?	Data-flow diagram / processing description
Why are they processed?	Purpose statement
Who can access them?	Access-control description
How are they secured?	Security documentation / controls
How long are they retained?	Retention/deletion terms
Are subcontractors involved?	Subprocessor disclosure and controls
What happens after contract expiry?	Return/deletion process
How are incidents handled?	Incident-response and notification procedure

17. Data Retention and Deletion: Educational institutions have legitimate reasons to retain some records for academic, legal, regulatory and administrative purposes. At the same time, indefinite retention of every digital record increases privacy and cybersecurity risk. Institutions should therefore create a documented retention schedule that distinguishes permanent academic records, legally required records, operational records and temporary information.

Record type	Illustrative governance approach
Degree/award records	Retain according to applicable academic and regulatory requirements.
Examination records	Retain according to university/regulatory record-keeping rules.
Financial records	Retain according to applicable tax, accounting and legal requirements.
Admission records	Define a documented period consistent with institutional/legal requirements.
CCTV	Define a proportionate period and secure access; preserve longer only when justified.
Temporary application data	Delete or anonymise when the relevant purpose and applicable retention requirement end.
Vendor copies	Require return/deletion according to contractual and legal requirements.

18. Personal Data Breach Management: A breach can arise from hacking, malware, lost devices, unauthorised disclosure, accidental email, weak access controls, compromised credentials, misconfigured cloud storage or inappropriate vendor access. Institutions should maintain a written incident-response plan and rehearse it periodically.

Suggested institutional workflow:

Stage	Action
1. Detect	Identify suspected loss, disclosure or unauthorised access.
2. Contain	Restrict accounts, isolate systems and stop further exposure.
3. Assess	Identify affected data, individuals, systems and likely consequences.
4. Escalate	Notify the designated institutional response team.
5. Notify	Make statutory notifications where required and within applicable timelines.
6. Remediate	Patch systems, reset credentials and correct the underlying weakness.
7. Document	Record decisions, evidence, actions and lessons learned.
8. Prevent	Update controls, training and vendor requirements.

19. Grievance Redressal and Data Principal Rights: The Act provides rights to Data Principals and requires an effective mechanism for grievance redressal.[1] Institutions should therefore create an accessible privacy contact or designated grievance mechanism and publish the relevant communication channel in institutional privacy notices. The mechanism should record the request, verify the requester where necessary, route it to the responsible department, record the response and provide escalation information where applicable.

A university may create a central privacy email/portal supported by a small internal committee comprising administration, IT, academic administration and legal/compliance personnel.

20. Proposed Institutional Governance Structure

Role	Core responsibility
Governing authority	Approve policy, resources and institutional accountability.
Data Protection / Privacy Committee	Coordinate policy, risk review, training and monitoring.
IT/Cybersecurity	Technical safeguards, access control, logging, backup and incident response.
Registrar/Administration	Records, notices, institutional procedures and coordination.
Examination section	Academic records, access control and retention.
Finance	Financial records and payment-related controls.
Faculty/Staff	Responsible day-to-day handling of student information.
Student welfare	Sensitive student-support information and controlled access.
Procurement/Vendor management	Data-protection requirements in contracts and due diligence.
Students/Parents	Use institutional systems responsibly and report concerns.

21. What is Mandatory for an Educational Institution? The word “mandatory” must be used carefully in a journal article because the DPDP Act has a phased commencement structure and some obligations may apply differently depending on the institution’s role and circumstances. The 13 November 2025 commencement notification specifies different dates for different provisions. Several core provisions, including sections 3–5 and 7–17, are scheduled to commence eighteen months after publication of the notification, while other provisions came into force on publication and additional provisions have a one-year commencement point.[1,16]

Accordingly, institutions should maintain a compliance register that distinguishes (a) provisions currently in force, (b) provisions scheduled to commence later, and (c) best-practice controls that the institution adopts proactively before the statutory deadline.

Compliance domain	Institutional action
Governance	Appoint accountable leadership and establish a documented privacy governance mechanism.
Data inventory	Map student, parent, staff and vendor personal data.

Notice	Prepare clear, standalone notices consistent with the Rules when applicable.
Consent	Implement consent and withdrawal mechanisms where consent is the applicable basis.
Children	Implement verifiable parental-consent and child-data safeguards where applicable.
Security	Implement reasonable technical and organisational safeguards.
Breach	Maintain a documented breach detection and response process.
Rights/grievance	Create an accessible mechanism for rights and grievance requests.
Retention	Create and periodically review retention/deletion schedules.
Vendors	Assess and govern third-party processing.
Training	Train faculty, staff and relevant students.
Audit	Periodically test compliance and security controls.

22. Penalty Provisions: The Schedule to the DPDP Act specifies maximum penalties for certain breaches. These amounts are statutory ceilings and should not be interpreted as automatic penalties imposed at the maximum level for every incident. The relevant authority considers the statutory framework when determining the penalty.[1]

Specified breach	Maximum penalty under Schedule
Failure to take reasonable security safeguards to prevent personal-data breach	Up to ₹250 crore
Failure to notify personal-data breach as required	Up to ₹200 crore
Breach relating to children's personal-data obligations	Up to ₹200 crore
Breach by a Significant Data Fiduciary of specified obligations	Up to ₹150 crore
Breach by a Data Principal of specified duties	Up to ₹10,000
Other breach of the Act / Rules	Up to ₹50 crore

23. Significant Data Fiduciary: The Act provides for a category of Significant Data Fiduciary (SDF) that may be notified by the Central Government based on factors including the volume and sensitivity of personal data, risk to the rights of Data Principals and other statutory considerations.[1] Educational institutions should not assume that every university automatically falls within this category. The institution should monitor government notifications and determine its obligations if it is notified or otherwise falls within a relevant category.

24. DPDP Rules, 2025 and Phased Commencement: The Digital Personal Data Protection Rules, 2025 were notified on 13 November 2025. The official Rules specify that Rules 1, 2 and 17–21 came into force on

publication; Rule 4 is scheduled to commence one year after publication; and Rules 3, 5–16, 22 and 23 are scheduled to commence eighteen months after publication.[2] The Act's corresponding commencement notification uses a phased structure as well.[16]

This staged approach is important for educational institutions preparing in 2026. A prudent institution can begin implementation immediately rather than waiting for each statutory commencement date. Early preparation reduces operational disruption and provides time for data mapping, procurement changes, privacy notices, training and system development.

25. Institutional DPDP Implementation Flowchart

Step	Implementation activity	Output
1	Leadership commitment	Institutional resolution / policy mandate
2	Data inventory	Master data register
3	Data-flow mapping	System and vendor data map
4	Purpose/legal basis review	Processing register
5	Privacy notice	Student/parent/staff notices
6	Consent management	Consent and withdrawal workflow where required
7	Child-data controls	Parent/guardian verification process where applicable
8	Security assessment	Risk register and security controls
9	Vendor review	Data-processing/vendor register
10	Retention/deletion	Retention schedule and deletion SOP
11	Breach readiness	Incident-response plan and escalation matrix
12	Rights/grievance	Request and complaint mechanism
13	Training	Faculty/staff/student awareness programme
14	Audit and improvement	Periodic compliance report

26. Institutional Compliance Checklist

No.	Control	Status (Yes/ No/ NA)	Evidence
1	Institutional data-protection policy approved	_____	Policy document
2	Data Protection/Privacy Committee identified	_____	Office order

3	Student data inventory completed	_____	Data register
4	Data-flow map completed	_____	Data-flow diagram
5	Privacy notices reviewed	_____	Published notices
6	Applicable consent process implemented	_____	Consent records
7	Child-data procedure implemented	_____	SOP / verification record
8	Role-based access implemented	_____	Access matrix
9	Security controls assessed	_____	Security audit
10	Vendor register completed	_____	Vendor register
11	Retention schedule approved	_____	Retention policy
12	Secure deletion process defined	_____	Deletion SOP/log
13	Breach response plan approved	_____	Incident-response plan
14	Grievance mechanism published	_____	Portal/email/SOP
15	Staff training completed	_____	Attendance/training record
16	Periodic review scheduled	_____	Annual review report

27. Model Data Governance Policy Structure

1. Purpose and scope
2. Definitions and institutional roles
3. Personal-data inventory and classification
4. Collection and purpose specification
5. Privacy notices and consent
6. Children's personal data
7. Access control
8. Information security
9. Third-party processors and vendors
10. Data retention and deletion
11. Personal-data breach response
12. Data Principal rights and grievance redressal

13. Staff and faculty responsibilities
14. Student and parent awareness
15. Audit and monitoring
16. Policy review and amendment

28. Challenges in DPDP Implementation

- Legacy paper and digital records may coexist, making data discovery difficult.
- Multiple software systems can create fragmented data flows.
- Institutions may lack dedicated privacy expertise.
- Faculty and administrative staff may have uneven awareness of data-protection responsibilities.
- Third-party educational technology providers may introduce additional data flows.
- Large institutions may have complex legacy access permissions.
- Retention and deletion can conflict with legitimate academic, regulatory or legal record-keeping needs.
- Child-data requirements may require new verification and system workflows.
- Smaller institutions may face resource constraints while implementing technical and organisational safeguards.
- Rapid adoption of AI-enabled educational tools creates additional questions about data use, vendor governance and responsible innovation.

29. Research Gap: Recent policy analysis has identified learner-data governance as an emerging issue in India and has noted that the DPDP Act provides a general framework rather than an education-sector-specific operational code.[8] International child-data research likewise highlights the need for multi-stakeholder governance, cybersecurity controls and practical guidance for schools and EdTech providers.[5-7,9] A significant research opportunity therefore exists for empirical studies examining how Indian schools, colleges and universities are translating statutory requirements into day-to-day procedures.

Future research should compare institutional readiness across government, aided and private institutions; examine parent and student awareness; study vendor contracts; evaluate consent workflows; and measure the effectiveness of data-breach preparedness and privacy training. Such studies could produce evidence-based sector-specific templates for India.

30. Recommendations

1. Develop sector-specific implementation guidance for educational institutions in coordination with relevant education regulators.
2. Create standard templates for privacy notices, consent workflows, child-data procedures, retention schedules and breach-response plans.

3. Establish institutional data inventories and data-flow maps before attempting advanced compliance automation.
4. Adopt role-based access control and review access rights at least periodically.
5. Include data-protection requirements in procurement and vendor contracts.
6. Conduct mandatory privacy and cybersecurity awareness programmes for faculty and administrative staff.
7. Create age-appropriate student awareness programmes on personal data, passwords, phishing and responsible digital behaviour.
8. Create a child-data governance procedure for institutions serving children.
9. Test breach-response plans through periodic tabletop exercises.
10. Maintain a statutory commencement tracker so that institutional implementation follows the phased legal timeline.
11. Integrate privacy governance into academic administration, student welfare, IT, procurement, finance and examination management.
12. Conduct periodic independent reviews of privacy and cybersecurity controls.

31. Discussion: The DPDP framework provides educational institutions with an opportunity to move from fragmented information-security practices toward structured data governance. The practical value of the law in education will depend not only on formal policies but also on whether institutions translate those policies into everyday behaviour. A privacy notice that students cannot understand, a consent mechanism that does not reflect actual processing, or an access policy that is not enforced provides limited protection.

The education sector also has a distinctive trust relationship. Students and parents generally provide information because the institution needs it to deliver education and related services. That relationship supports an expectation that data will be handled responsibly. UNICEF's education-focused privacy guidance emphasises the importance of safeguards, governance and cybersecurity when educational technology is used with children.[5-7] Indian institutions can adapt these principles to the DPDP framework while recognising the specific statutory structure of Indian law.

The phased commencement of the Act and Rules should be understood as implementation time, not as a reason to postpone governance. Early data mapping and security improvements can be undertaken before all provisions become operational. Institutions that begin with basic governance—knowing what data they hold, why they hold it, who can access it and when it should be deleted—can then build more advanced compliance mechanisms.

32. Conclusion: The Digital Personal Data Protection Act, 2023 is highly relevant to the modern educational institution because education has become deeply dependent on digital personal data. Student information is used across admission, attendance, examinations, finance, learning systems, communication, welfare and other institutional functions. The resulting data environment creates responsibilities concerning lawful processing, transparency, security, children's data, grievance redressal and responsible relationships with technology vendors.[1,2]

Children's data requires particular attention because the Act defines a child as a person who has not completed eighteen years and establishes additional requirements for children's personal data.[1]

Educational institutions should therefore create child-specific procedures for age identification, verifiable parental or lawful-guardian consent where required, appropriate use, security, vendor controls and retention.

The statutory penalty framework, including maximum penalties of up to ₹250 crore for specified failures concerning reasonable security safeguards, reinforces the importance of institutional preparedness.[1] However, compliance should not be reduced to avoiding financial penalties. Responsible data governance can strengthen student trust, administrative discipline, cybersecurity and institutional accountability.

Educational institutions should consequently establish an institution-wide implementation programme involving leadership, administration, IT, faculty, examination, finance, student welfare, procurement, vendors, students and parents. A structured data inventory, purpose map, privacy notice, access-control matrix, retention schedule, breach-response plan, grievance mechanism and periodic audit can provide the practical foundation for implementation. Because the Act and Rules have phased commencement dates, institutions should maintain a current legal-compliance tracker and update their policies as provisions become operational.[1,2,16]

In conclusion, DPDP compliance in education should be viewed as a continuous governance process: identify data, understand its purpose, protect it, limit access, retain it appropriately, respond responsibly to incidents and respect the rights of Data Principals. Such a framework can support digital innovation in education while strengthening privacy, trust and institutional responsibility.

33. Limitations

- This is a legal and policy review rather than an empirical survey of Indian educational institutions.
- The article does not claim that every institution has identical statutory obligations.
- The DPDP Act and Rules have phased commencement; institutional obligations should be checked against the applicable commencement notifications at the time of implementation.
- Sector-specific laws, regulations, contractual requirements and accreditation conditions may impose additional record-keeping or privacy requirements.
- This article is for academic information and is not a substitute for institution-specific legal advice.

34. Suggested Future Research

1. Survey DPDP readiness among Indian universities and colleges.
2. Compare privacy awareness among students, parents, faculty and administrators.
3. Study the effectiveness of parental-consent mechanisms for children's data.
4. Examine privacy clauses in educational-technology vendor contracts.
5. Develop and validate an Educational Institution DPDP Readiness Index.
6. Evaluate data-breach preparedness through institutional simulations.
7. Study the governance of AI-enabled learning platforms and student analytics.
8. Develop model data-retention schedules for different categories of educational records.

35. References

1. Government of India. The Digital Personal Data Protection Act, 2023. Act No. 22 of 2023. New Delhi: Gazette of India; 2023.
2. Ministry of Electronics and Information Technology, Government of India. Digital Personal Data Protection Rules, 2025. G.S.R. 846(E). New Delhi: MeitY; 2025.
3. Ministry of Electronics and Information Technology, Government of India. Explanatory Note to the Digital Personal Data Protection Rules, 2025. New Delhi: MeitY; 2025.
4. Ministry of Electronics and Information Technology, Government of India. Enforcement timeline for the Digital Personal Data Protection Act. New Delhi: MeitY; 2025.
5. UNICEF Europe and Central Asia. Data protection in schools: guidance for legislators, policy makers and schools. New York: UNICEF; 2024.
6. UNICEF Innocenti. Governance of student data: evidence, gaps, unanswered questions and recommendations for policymakers, educators, civil society and tech companies. Florence: UNICEF Innocenti; 2025.
7. UNICEF Innocenti. Data governance for EdTech: landscape review and policy recommendations. Florence: UNICEF Innocenti; 2025.
8. Tulsyan A. Governing learner data risks in India: the DPDP Act and the case for EdTech-specific regulation. Observer Research Foundation Issue Brief No. 879. New Delhi: ORF; 2026.
9. UNICEF. Children and online privacy. New York: UNICEF; 2019.
10. UNICEF. Child protection in digital education: policy brief and technical note. New York: UNICEF.
11. Ministry of Education, Government of India. National Education Policy 2020. New Delhi: Ministry of Education; 2020.
12. Government of India. Constitution of India. New Delhi: Legislative Department, Ministry of Law and Justice.
13. Supreme Court of India. Justice K.S. Puttaswamy (Retd.) v Union of India. (2017) 10 SCC 1.
14. Government of India. Information Technology Act, 2000. Act No. 21 of 2000. New Delhi: Government of India.
15. Ministry of Electronics and Information Technology. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. New Delhi: MeitY; 2011.
16. Ministry of Electronics and Information Technology, Government of India. Notification appointing commencement dates under the Digital Personal Data Protection Act, 2023. G.S.R. 843(E). New Delhi: MeitY; 2025.
17. Ministry of Electronics and Information Technology, Government of India. Notification establishing the Data Protection Board of India. G.S.R. 844(E). New Delhi: MeitY; 2025.
18. UNESCO. Global Education Monitoring Report 2023: Technology in education—A tool on whose terms? Paris: UNESCO; 2023.
19. UNESCO. Guidance for generative AI in education and research. Paris: UNESCO; 2023.

20. UNESCO. Recommendation on the Ethics of Artificial Intelligence. Paris: UNESCO; 2021.
21. UNICEF. Policy guidance on AI for children. New York: UNICEF; 2021.
22. OECD. Education at a glance 2024: OECD indicators. Paris: OECD Publishing; 2024.
23. OECD. Digital education outlook 2023: towards an effective digital education ecosystem. Paris: OECD Publishing; 2023.
24. European Union. Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union. 2016.
25. Information Commissioner's Office. Data protection and children. Wilmslow: ICO.
26. Council of Europe. Guidelines on children's data protection in an education setting. Strasbourg: Council of Europe.
27. World Economic Forum. Global cybersecurity outlook 2025. Geneva: World Economic Forum; 2025.
28. National Institute of Standards and Technology. Cybersecurity framework 2.0. Gaithersburg (MD): NIST; 2024.
29. International Organization for Standardization. ISO/IEC 27001:2022 information security, cybersecurity and privacy protection—Information security management systems—Requirements. Geneva: ISO; 2022.
30. International Organization for Standardization. ISO/IEC 27701:2019 security techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management. Geneva: ISO; 2019.

36. Official / Supporting Web Sources

1. India Code – Digital Personal Data Protection Act, 2023: <https://www.indiacode.nic.in/>
2. MeitY – Digital Personal Data Protection Rules, 2025: <https://www.meity.gov.in/>
3. MeitY – Act and Policies: <https://www.meity.gov.in/documents/act-and-policies>
4. UNICEF – Data protection in schools: <https://www.unicef.org/eca/reports/data-protection-schools>
5. UNICEF Innocenti – Data governance for EdTech: <https://www.unicef.org/innocenti/reports/data-governance-edtech>
6. UNICEF Innocenti – Governance of student data: <https://www.unicef.org/innocenti/reports/governance-student-data>
7. UNESCO – Global Education Monitoring Report 2023: <https://www.unesco.org/gem-report/en/technology>
8. Observer Research Foundation – Learner data risks in India: <https://www.orfonline.org/research/governing-learner-data-risks-in-india-the-dpdp-act-and-the-case-for-edtech-specific-regulation>

Citation: Pradhan. A., (2026) “Importance of the Digital Personal Data Protection (DPDP) Act, 2023 for Educational Institutes in India”, *Bharati International Journal of Multidisciplinary Research & Development (BIJMRD)*, Vol-4, Issue-08, August-2026.