



Source: AI Generated Image by ImagineArt and edited with Canva

Date published: July 13, 2025

Deploying Responsible AI (Ed-Tech Applications) in Indian Schools: Key Measures Towards Preserving Privacy Data of Children

Author: Ms. [Jayasri Ananthapadmanaban](#)

Reviewed by: Mr. [Vijayakumar A](#), Ms. [Choodamani V](#) and Mr. [Solomon Sagayaraj J MBA,CISA,CISM,CGEIT,CRISC,CDPSE](#)

Introduction

The integration of Artificial Intelligence (AI) into the Indian school system offers the promise of personalized learning, improved administrative efficiency, and inclusive education. However, the growing deployment of AI-based Ed-Tech tools in schools has raised pressing concerns around the privacy of children.

With children increasingly becoming data subjects—often without informed consent—the need for deploying **Responsible AI** with **Child-centric AI Governance** is of paramount importance to Indian schools.

This article explores how Indian schools can adopt sound AI practices ensuring data dignity, equity, and safety of children.

AI Use-Cases in Ed-Tech for Schools – Privacy Risks & Harm

With AI being a boon in several cases, they have risks associated with them equally. The below tables tries to capture the common use-cases in the EdTech mapped with Privacy risks and Harms to Children / Parents.

Use-Case	Functionality	🚫 Privacy Risks for Children	🔥 Harms to Children / Parents
Personalized Learning Paths	Adaptive content based on learning style and pace	Profiling based on behavioral data	Labeling of abilities; Peer Pressure; Biometric misuse
Predictive Dropout Detection	Flags risk of disengagement	Aggregated historical and socio-economic data	Labeling students as "at risk"; discrimination
Automated Assessments & Feedback	AI evaluates and gives real-time feedback	Algorithmic bias in scoring	Unfair grading due to algorithmic bias; decreased teacher involvement
Speech & Language Assistants	Voice-based practice and feedback	Voice recordings and usage metadata	Misinterpretation of speech; over-collection of sensitive data
Assistive Tech for specially-abled	AI-powered tools for diverse needs	Excessive data retention about impairments; Profiling and Labeling; Secondary use without consent	Surveillance Harm – reducing children's autonomy or self-expression. Parents may not be aware how to request deletion or correction of historical data; Future exclusion from services or opportunities based on the impairment data being shared or inferred
Classroom Behavior Monitoring	Detects behavior deviations	Surveillance of student actions	Normal behaviors misunderstood; embarrassment or bias

Applicable Indian Laws and Standards

As always, there are plenty of Laws / Frameworks that will be applicable to the EdTech Industry, the below tables summarise the relevant provisions from the law / framework.

Law/Framework	Relevant Provisions
DPDPA, 2023	Aims to safeguard individual privacy by driving transparency, ensuring accountability in data handling, and giving citizens control over their personal data
IT Rules, 2021	Mandates transparency by intermediaries and EdTech platforms
NEP 2020	Supports responsible tech in education with ethical guidelines
RTE Act	Ensures children's rights to safe and inclusive education
UNCRC	Right to privacy and protection from exploitation
ISO/IEC 42001	AI Management Systems – transparency, explainability, governance
ISO/IEC 27701	Privacy Information Management, linked to PII safeguards
ISO/IEC 22989 & 23894	Risk and bias management in AI systems

AI Use-Cases in Ed-Tech for Schools – Regulatory & Standards Mapping

Regulations and Standards are an important consideration before implementing an AI based solution at Schools.

In a nutshell,

- **DPDP Act 2023** establishes **child data as sensitive**, requiring **strict consent, lawful processing, and parental involvement**.
- **NEP 2020** supports AI and digital learning only when **inclusive, ethical, and pedagogically beneficial**.
- **ISO/IEC 42001** provides AI-specific **risk governance, transparency, and lifecycle oversight standards**

The below table provides the regulation / standard requirement against few common use-cases in the Ed-Tech industry.

Use-Case	India DPDP Act (2023)	NEP 2020	ISO/IEC 42001 (AI MS)
Personalized Learning Paths	Data minimization, consent (Section 6), child-centric safeguards	Competency-based and personalized learning (NEP Sec. 4.4, 4.5)	Clause 6.3: Risk assessment on AI personalization
Predictive Dropout Detection	Guard against profiling; explainability and fairness are mandatory	Identify at-risk learners for early support (Sec. 6.6)	Clause 6.2.2: Mitigate algorithmic bias
Automated Assessments & Feedback	Section 7(c) – Legitimate use; Section 9(1)(b) – Storage limitation; Section 9(5) – Processing of children’s data; Section 6(1)(a) – Notice requirement	Encourages automated yet fair assessments (Sec. 4.34, 4.38)	Clause 7.4: Algorithmic decision management
Speech & Language Assistants	Sensitive personal data (biometric/voice) – Voice + Video capture of Children is biometric and special category data; parental consent required	Inclusive tools for special education (Sec. 4.27)	Clause 6.4.4: Impact of AI on vulnerable groups
Assistive Tech for specially-abled.	Enhanced protections for specially abled children; ensure accessibility	Strong support for inclusion (Sec. 6.6, 4.27)	Clause 8.2.2: AI fairness for differently-abled users
Classroom Behavior Monitoring	Section 9 (3) A Data Fiduciary shall not undertake tracking or behavioural monitoring of children or targeted advertising directed at children.	Behavioral insights encouraged but with teacher oversight (Sec. 4.25)	Clause 6.4.3: Oversight of AI in monitoring environments

Key Stakeholders & Responsibilities

The below tables summarises the key stakeholders and their responsibilities for the AI eco-system based setup at EdTech:

Stakeholder	Responsibilities
Ed-Tech Developer	Build AI systems with fairness, Human-In-The-Loop, and documentation (e.g., model cards); bias audit
School/Deployer	Obtain consent, explain systems to parents/teachers/students, manage governance
Parents/Guardians	Understand data use and provide informed consent
Students	Engage in safe tech usage; understand rights
Government/Board	Enforce policy and ethics audits in EdTech vendors
DPBI – Data Protection Board of India / Regulators	Set child-specific guidelines and oversee penalties for non-compliance

AI Lifecycle - Roles in Safeguarding Children's Privacy

The below tables summarises the role of key stakeholders during various stages of the AI Lifecycle and their relevant standard / guideline mapping:

Phase	Developer	School/Deployer	Standards/Guidelines
✦ Phase 1: Governance & Planning	Include privacy by design in requirement gathering	Define governance policy on AI use	ISO 42001 Clauses 5–6; DPDPA Sections 3, 9
✦ Phase 2: Data Collection & Preprocessing	Collect only relevant child data (data minimization)	Obtain verifiable parental consent	DPDPA Sec. 9, ISO 27701, IT Rules 2021
✦ Phase 3: Model Training and Test, Evaluation, Verification and Validation[TEVV]	Conduct bias audit, use Human-In-The-Loop [HITL]	Review Test, Evaluation, Verification and Validation reports and question anomalies	ISO 22989 (risk categorization), ISO 23894 (bias mitigation)
✦ Phase 4: Deployment & Classroom Use	Document model limitations, share explainability tools	Train teachers on AI tool limitations and ethics	ISO 42001 Clause 9, GDPR Art. 22 (analogous)
✦ Phase 5: Post-Deployment Monitoring	Enable continuous drift detection, feedback channels	Set up periodic audits and parental reporting tools	ISO 42001 Clause 10 (PMS), DPDPA logs and reporting duties

Advice to Stakeholders: Ensuring Children’s Privacy

The below provides guidance on how to ensure Children's Privacy while carrying our different roles:

Who	Action Required to Protect Children’s PII
Schools [Deployer]	<ul style="list-style-type: none"> - Create privacy and AI use policy - Conduct EdTech vendor due diligence - Ensure purpose-specific usage - Appoint a privacy coordinator - Collect and manage verifiable parental consent - Avoid unnecessary data like emotional analytics unless justified
Ed-Tech Providers [Developer]	<ul style="list-style-type: none"> - Limit data collection - Document explainability - Build parental dashboards - Apply age-appropriate design
Parents/Guardians	<ul style="list-style-type: none"> - Ask how data will be used - Request opt-outs - Read and question EdTech policies
Regulators	<ul style="list-style-type: none"> - Develop child-specific AI standards for schools - Mandate Data Privacy Impact Assessment [DPIAs] or Fundamental Rights Impact Assessment [FRIAs] for EdTech tools - Mandate Attestation for EdTech tools before deployment either directly by Regulators or body appointed by Regulators - Enforce clear enforcement pathways for misuse

Conclusion

Responsible AI in Indian schools is not a luxury—it is **an ethical and legal necessity**. Children deserve technology that supports learning **without compromising their privacy or autonomy**.

With the **DPDPA, NEP in force**, and global AI & privacy benchmarks guiding standards, it's time to align India's fast-growing EdTech sector and schools with **Child-Centric AI Governance** – a structured, ethical, and rights-based approach to designing, deploying, and overseeing AI systems that directly or indirectly affect children.

|"In protecting a child's data today, we preserve their dignity tomorrow."

References:

1. Digital Personal Data Protection Act, 2023. Government of India.
2. National Education Policy, 2020. Ministry of Education, India.
3. UNICEF (2021). *Policy Guidance on AI for Children*.
4. NITI Aayog (2018). *National Strategy for Artificial Intelligence*.
5. OpenMined. <https://www.openmined.org>
6. TensorFlow Privacy. Google Research.
7. OECD (2019). *Principles on Artificial Intelligence*.
8. Mozilla Foundation. *Creating Trustworthy AI*
9. Inclusive Education with AI: Supporting Special Needs and Tackling Language Barriers - <https://arxiv.org/html/2504.14120v1>

About this AI and Privacy Research newsletter series:

<https://www.linkedin.com/pulse/introduction-newsletter-series-ai-privacy-research-xf0ec/>