

HOME / EDUCATION

# India's AI revolution in education: Promise, peril, and the search for balance



Updated - November 12, 2025 06:40 pm IST

O.R.S. RAO



India's national approach to AI governance established under the IndiaAI Mission, adopts a conscious philosophy of promoting responsible AI usage while avoiding statutory overreach and without stifling innovation. | Photo: iStock/ Getty Images

The adoption of Artificial Intelligence (AI) in India's education sector, particularly by students, is galloping faster than anybody could predict. As India gears up to introduce AI education from Class 3 from 2026–27, the rapid, large-scale deployment presents a governance challenge. This comes against the backdrop of the surge in misuse of AI, in areas such as academic dishonesty, deepfakes, manipulated images, and the consequent psychological harm to young people. This article examines India's recently announced governance guidelines on AI use, drawing

comparisons with the prevailing governance models, in the world and proposes a framework to safeguard educational integrity and digital safety for the next generation.

## **India's AI governance guidelines : balancing regulation and innovation**

India's national approach to AI governance established under the IndiaAI Mission, adopts a conscious philosophy of promoting responsible AI usage while avoiding statutory overreach and without stifling innovation. The policy guidelines announced by the Government of India on November 5, 2025, are based on a report submitted by a committee of experts chaired by Prof. B. Ravindran of IIT Madras, in July this year.

The report proposed a flexible and phased governance model built upon seven guiding principles: trust; people first (emphasising human oversight); fairness and equity (mandating inclusion and preventing discrimination); accountability (establishing clear responsibility); understandable by design (requiring transparency); and safety, resilience, and sustainability (ensuring robust security). The report recommended that a separate, standalone law to regulate AI is "not needed at this stage", given the current assessment of risks. Hence, the proposed governance structure relies on leveraging existing statutes — the Information Technology Act, 2000, the Bharatiya Nyaya Samhita, and the Digital Personal Data Protection (DPDP) Act, 2023.

The proposed architecture features a trio of new oversight bodies: the AI Governance Group (AIGG), which will coordinate across various ministries, regulators, and standard-setting agencies to promote access to AI safety tools; the Technology and Policy Expert Committee (TPEC), responsible for strategic oversight, review of laws, and suggesting reforms; and the AI Safety Institute (AISi), focused on technical validation and safety research. The governance guidelines are supported by an Action Plan that maps key recommendations across short, medium, and long-term timelines.

As the impact of AI is different for each sector, the sectoral regulators and bodies are expected to study the impact of AI in the respective sector and amend or adapt its laws accordingly, under the oversight of the inter-ministerial body, AIGG. Interestingly, while the key agencies for Banking, Financial Services, Insurance, Telecom and Healthcare sectors were listed in the guidelines, education sector does not find a mention.

## **Need for speeding up regulations**

While the approach of light regulation will enable unhindered innovation in the burgeoning field of AI, the policy of phased governance may create a critical pacing problem, wherein AI adoption is advancing faster than institutional readiness. This gap between widespread student use and lack of readiness of institutional governance is likely to create an environment ripe for

unregulated adoption, undermining academic integrity and leading to unintended delirious consequences for the students and the society as a whole. The most compelling arguments for regulatory urgency stem from the documented cases of AI, being weaponised for social and psychological harm among youngsters, extending far beyond the classroom.

## Academic misuse

In a landmark shift in policy, the University Grants Commission (UGC), in September 2025 approved the use of AI tools in education, wherein students can now leverage AI for research, data analysis, presentations, and project development. This move comes with crucial ethical guardrails with regard to citation of AI created content and the universities are expected to monitor “over-reliance” of the students on AI. However, the challenge remains in establishing detection and enforcement standards that can keep pace with the technology. Recent studies have shown that over 20% of students admitted to using or copying output from AI chatbots for academic work, but only about one AI misuse case in almost 400 students was penalised.

## Cases of Digital Harm

In October 2025, a student at IIIT Naya Raipur was expelled for using AI tools to morph and distribute obscene images of more than 35 female classmates. Devices were seized, and an FIR was filed against the individual, revealing how AI is being weaponised for harassment and privacy invasions, reaffirming the regulatory imperative.

The risks inherent in unregulated Generative AI are amplified in the realm of emotional and mental health, as illustrated by the tragic case of the 14-year-old American teenager who took his own life after forming an intense emotional attachment to an AI chatbot. His family attributed the death to the AI tool. His family laid blame on the AI tool for his death.

The subsequent investigations of the chat transcripts revealed intimate conversations in which the chatbot discussed suicide. In another case, the family of a 16-year-old American filed a wrongful death lawsuit against OpenAI earlier this year, alleging that the company prioritised deepening its users’ engagement with ChatGPT over safety. These cases serve a stark warning on how highly engaging Generative AI, particularly companion bots, can foster deep emotional dependency, overriding human judgment and actively encouraging self-harm.

## Experience of the other countries

The European Union has established the world’s first comprehensive legally binding framework, the AI Act, which follows a prescriptive approach rooted in the precautionary principle, aims primarily to safeguard fundamental rights, health, and safety. It employs a strict three level risk-based classification system: unacceptable, high, and limited risk.

AI tools with unacceptable risk, which pose clear threats to human safety, livelihoods, or rights are banned. High risk systems, which profile individuals or operate in critical sectors like healthcare, employment, or law enforcement are heavily regulated. AI applications, such as chatbots and deepfakes, that present limited risk require lighter transparency obligations, primarily ensuring awareness of the end-users. The AI Act came into force in August 2024, with full applicability to be phased over two years. The EU model is often described as compliance-heavy and prescriptive.

Unlike Europe, the U.S. has no comprehensive federal AI law, instead relying on a blend of State-level policies, sector-specific regulations, and Presidential Executive Orders. In 2024 alone, over 700 bills addressed AI, with the States of California, Colorado, New York, and Texas, leading legislative efforts. After investigating into allegations over AI chatbot companies, the U.S. Federal Government, in October 2025, proposed the Guard Act, which intends to mandate robust age verification for users of Generative AI companies. As a result, most of these companies are planning to immediately implement age verification and prohibit minors under 18 years to access companion chatbots.

Other countries—U.K., Japan, China—are also advancing their regulatory frameworks, each balancing trust, innovation, and risk management, in distinct ways.

In response to the global need, the AI Education Framework v1.0, published in July 2025, by AI Governance Network (AIGN), offers a prescriptive architecture for systematic remediation, based on Global Maturity Index (GMI) for governance. Four tiers are defined: Initial, Defined, Managed and Optimised. By achieving higher tiers, institutions establish trust in the ethical and secure handling of data by their partners and vendors globally.

## **Charting a future-proof regulatory framework**

India's path toward responsible AI in education needs a regulatory framework based on the risk assessment of AI in education sector. The proposed AI Governance Group (AIGG) and Technology & Policy Expert Committee (TPEC) must urgently define a clear liability regime for algorithmic failures. Given the "hallucination crisis" where AI-generated lesson plans can be instantly deployed without formal scrutiny, the policy must clarify accountability, when factual errors or algorithmic bias led to a student's failure. Targeted legal amendments must provide clarity beyond the general application of the IT Act.

Considering the large scale exposure of students' personal data to EdTech and digital marketing companies, the Digital Personal Data Protection (DPDP) Act must be rigorously enforced against third-party Ed-Tech vendors, mandating frequent, independent security audits and imposing substantial financial penalties for non-compliance. This is the primary mechanism for

upholding the foundational principle of “people first” and protecting sensitive student data from the possibility of misuse.

India must move beyond general training by standardising faculty development programs into a cohesive national curriculum that includes not only AI awareness but also modules on Responsible AI.

## Conclusion

India stands at a pivotal juncture, ready to harness the vast potential of AI to transform education and leapfrog into a digital economy. However, any unchecked misuse of this cutting-edge technology can result in serious consequences—from deepfake harassment targeting young women, to ethical ambiguities of mass plagiarism and the tragic risks associated with emotional AI systems.

The country’s current “Innovation over restraint” philosophy, while essential for driving quick AI innovation and adoption, warrants supplementation with a mandatory safety framework. By rapidly operationalising its new institutional bodies, enforcing rigorous vendor accountability, India can ensure that its technological advancement is secured by ethical, protective, and human-centric governance. The time for voluntary guidelines is over; the era of enforceable guardrails must begin now. While AI needs to be harnessed to the hilt, AI security is equally important to ensure the academic integrity and safety of the students.

*(Prof O.R.S. Rao is the Chancellor of the ICFAI University, Sikkim. Views are personal)*

*Those in distress or having suicidal tendencies could seek help and counselling by calling any of the following numbers:*

Published - November 12, 2025 06:39 pm IST

---

## Related Topics

[education](#) / [Artificial Intelligence](#)

THE  HINDU

The Hindu

About Us

Code of Editorial Values