

INDIA TODAY

Is the APAAR ID safe? CBSE's permanent academic record and student privacy concerns

A single ID promises to simplify a child's academic journey: no lost records, no repeated paperwork, just one digital trail. But when that trail becomes permanent, it also raises deeper questions about privacy, control, and long-term impact. The real question is: are we ready to trade convenience for lifelong data visibility?



A single ID promises to simplify a child's academic journey. The real question is: are we ready to trade convenience for lifelong data visibility? (Image: AI-generated)

What if your entire school life, every mark, every certificate, every achievement, was stored in one permanent digital record?

That is what CBSE's APAAR system is building: a single, centralised academic ID that could shape everything from school transfers to college admissions and job verification.

It promises a future with no lost documents and seamless access to records. But it also creates something India has struggled with before: a massive, centralised database of personal data.

The Ministry's official APAAR site portal asks for detailed personal data such as name, date of birth, gender, mobile number, parents' names, Aadhaar-linked name and Aadhaar number. That is a lot of information for one school record, and it is exactly why privacy questions are not alarmist, but necessary.

Because when a child's academic identity becomes permanent and digital, The question is not just about convenience, but about control, security, and long-term consequences.

APAAR is no longer just a policy idea. It is already becoming part of how schools function. CBSE has called it the "primary identifier" for students in affiliated schools. It is also being linked to board processes like LOC submissions for Classes 10 and 12.

So what exactly is it?

According to the official APAAR portal, it is a 12-digit unique ID that stores a student's academic journey: marksheets, degrees, diplomas, certificates, even co-curricular achievements.

WHY APAAR LOOKS USEFUL, AND WHY IT WORRIES PARENTS

India has seen the power, and the risks, of large digital identity systems before.

Over the years, Aadhaar-linked databases have faced multiple data exposure concerns. In 2017, reports suggested that details of over 130 million bank accounts linked to Aadhaar were leaked through government websites.

More recently, in 2023, a massive breach reportedly exposed personal data of over 81 crore Indians, including Aadhaar-related information, in what was described as one of the largest data leaks in the country.

These incidents did not just raise questions about technology, they raised concerns about how securely large, centralised databases are managed.

That is exactly why APAAR is being watched closely.

On paper, the system is designed to simplify education. The Ministry says it will make school transfers smoother, reduce paperwork, prevent duplication, and allow students to carry their academic records seamlessly across institutions.

The process, too, appears structured. The ID is created after school verification, authentication, and parental consent, and then stored in DigiLocker for secure access.

But the scale of data being collected tells another story. To generate a single APAAR ID, the system requires detailed personal information, from basic identity details to Aadhaar-linked data and parental information.

And that brings back a familiar concern: When so much sensitive data sits in one place, how safe is it really?

Manisha Malhotra, Director-Principal of Satya School, Gurugram, sees APAAR as part of India's broader digital shift, similar to how Aadhaar transformed identity systems.

But she also adds a note of caution:

"Whenever we create a permanent digital academic record, concerns around data protection, access, and potential misuse are valid and must be addressed seriously." Her point reflects what many parents are beginning to feel. The idea of APAAR may be efficient. But trust will depend not on what it promises, but on how securely it is built, managed, and explained.

WHAT THE LAW DEMANDS

That trust has a legal backbone too. The Digital Personal Data Protection Act, 2023 says consent must be "free, specific, informed, unconditional and unambiguous".

It also says that before processing a child's personal data, the data fiduciary must obtain verifiable parental consent. The law further bars tracking or behavioural monitoring of children and targeted advertising directed at them.

In other words, child data is not supposed to be treated like ordinary data. It comes with stronger duties and tighter limits.

Dr Sanjay Katkar, Joint Managing Director of Quick Heal Technologies, warned that the real danger lies in centralisation. A lifelong ID, he said, can gather years of marks, demographic details and other sensitive information in one place. If that system is breached or misconfigured, "an entire generation's records" could be exposed.

He also flagged "function creep", where data collected for one purpose slowly gets reused for others that parents never agreed to, such as screening, profiling or future decisions unrelated to schooling.

THE REAL RISK IS NOT JUST HACKS, BUT MISUSE

The APAAR portal presents the ID as a tool for accountability, transparency, and student mobility. But by creating a permanent, centralised trail, it also raises deeper concerns.

A child's academic record should not become a lifelong label. Dr Sanjay Katkar warns that every student must retain the right to "evolve, make mistakes, and start with a clean slate."

Without strict limits on purpose and access, a permanent record could quietly transform into a comprehensive profile rather than a school aid, showing not just grades, but skills, interests, and school choices.

In a worst-case scenario, such data could be exploited by third parties, like corporates or institutions, to make pre-judged decisions, shaping admissions, scholarships, or recruitment opportunities before a child has even made independent choices.

This is why implementation matters as much as policy.

CBSE circulars show that APAAR is already tied to school registration and board processes, highlighting the need for clear access rules, defined retention periods, and explicit consent mechanisms.

Parents must know exactly who can access the data, for how long, and for what purpose. Schools need simple, transparent grievance channels.

And the system itself should be backed by tested technical safeguards, including encryption, role-based access, and independent audits, not just promises on paper.

Without these practical protections, convenience could come at the cost of privacy, fairness, and a child's future opportunities.

WHAT SAFEGUARDS SHOULD DECIDE APAAR'S FUTURE

Malhotra said the framework must rest on “secure digital infrastructure, controlled access, and authenticated data sharing.” She stressed that the intent may be to streamline transfers and prevent fraud, but the proof will lie in execution.

Dr Katkar made a similar case, arguing for strong encryption, role-based access, audit trails and independent security checks as the minimum starting point.

That is the heart of the APAAR debate. A permanent academic record can reduce friction in schools and make certificates easier to verify.

But if the safeguards are weak, convenience can come at the cost of a child's privacy, dignity and future choice. For a system built around children, that question cannot be left to technology alone.

- Ends