SUMS+
Education Management System

SUMS ERP + Siccura Discover · Consent · Regula

DPDP Act 2023 | Education Compliance Guide

A Compliance Guide for Educational Institutes

Schools • Colleges • Universities • Coaching Classes

WHAT'S INSIDE

01. Why DPDP Act 2023 matters for education

The Digital Personal Data Protection Act, 2023 (DPDP Act) is India's first comprehensive personal data protection law. It applies to any organisation that collects, stores or processes the personal data of individuals in India — and that includes every educational institute.

Education is the highest-risk sector under the DPDP Act for one simple reason: most learners are minors. The Act defines a child as anyone under the age of 18 and imposes special obligations on any Data Fiduciary that processes a child's personal data.

Personal data that schools, colleges and coaching classes routinely handle

Student name, photograph, date of birth, address, Aadhaar/ID, parent and guardian names with contact details, medical records, fee and payment information, attendance, marks and assessments, transport and hostel records, library activity, online learning behaviour, scholarship and financial-aid information, alumni records. Each of these is personal data under the Act, and most of it belongs to a minor.

What the law specifically demands when minors are involved

- Verifiable consent of the parent or lawful guardian must be obtained before any processing of a child's data.
- No tracking or behavioural monitoring of children is permitted.
- No targeted advertising may be directed at children.
- Notice to parents must be in clear, plain language and available in English plus any language in the Eighth Schedule.
- Parents must be able to withdraw consent, view, correct and request erasure of their child's data.
- All security obligations of a Data Fiduciary apply equally — reasonable safeguards, breach notification, audit-ready records.

Maximum penalties (Schedule of the Act)

- Up to Rs. 200 crores for breaches of children's data obligations.
- Up to Rs. 250 crores for failing to implement reasonable security safeguards.
- Up to Rs. 200 crores for failing to notify the Data Protection Board or affected parents of a breach.
- Up to Rs. 50 crores for any other breach of the Act.

02. Top DPDP risks common in schools, colleges & coaching

Most institutes already do many of these things every day without realising they are now regulated activities under the DPDP Act. Here are the most common risk patterns we see:

Student photos and videos circulated freely — class photos, event videos and student work posted on WhatsApp parent groups, the website and social media without verifiable parental consent for the specific purpose.
Open student data files — Excel sheets with full student lists, dates of birth, parent phone numbers, addresses and fee status circulated freely between staff and external vendors with no access control.
Marketing outreach using parent data — numbers and emails collected for fee reminders reused for promotional SMS, edtech pitches or fundraising — without fresh consent for that purpose.
Unmanaged vendor and partner data sharing — transport, canteen, photographers, exam bureaus, edtech platforms and SaaS tools receiving student lists with no written contract, no security obligations and no erasure clause.
Long-tail retention with no purpose — records of students who left years ago still sitting in shared folders, old hard drives and personal staff laptops with no retention schedule or erasure trigger.
Behavioural tracking inside student-facing apps — third-party analytics, ad trackers and engagement scoring enabled by default on apps and websites used by students under 18 — directly prohibited by the Act.

03. The 7-step DPDP compliance roadmap for education

Follow these seven steps in order. Each is mapped to the relevant area of the DPDP Act and includes a real example from the education sector.

1	**Discover & map your data** Identify every place personal data lives — admission forms, ERP, fee software, library, transport register, medical records, photo galleries, staff laptops, shared drives, WhatsApp groups, cloud folders. Classify each record by sensitivity. ***Example:*** *A school discovers Aadhaar photocopies in three cupboards, an Excel of parent phone numbers on the receptionist's PC, and a Google Drive folder of five years of class photos shared publicly.*
2	**Build notice & consent into admission and every new use** Provide a plain-language notice at admission stating what data is collected, why, how parents exercise rights, and how to complain to the Board. Obtain verifiable parental consent, and a fresh consent for any new purpose. ***Example:*** *A coaching class adds a structured consent form at admission — separate boxes for academic communication, fee communication, photos on social media, and sharing with an edtech partner. Each parent ticks each box independently.*

3	**Protect children's data with extra care** For every learner under 18, obtain verifiable parental consent before processing. Stop all tracking, behavioural profiling and targeted advertising directed at children. Disable third-party trackers on student-facing apps and websites. ***Example:*** *A college's exam-prep portal previously used a third-party analytics SDK to measure engagement. For all users below 18 this is disabled and replaced with a privacy-respecting alternative.*
4	**Secure data with reasonable safeguards** Implement technical and organisational measures: role-based access, protection that travels with sensitive files, secure sharing, endpoint protection, classification by sensitivity, secure deletion when no longer needed. Train staff regularly. ***Example:*** *A university classifies all student records as Confidential; files on staff laptops carry their protection with them; sharing with external assessors uses view-only links; teachers complete a 30-minute DPDP module each year.*
5	**Honour parent and student rights** Provide easy ways for parents and adult students to view a summary of data held, correct mistakes, request erasure, raise grievances and nominate someone in case of incapacity. Respond within the prescribed timeline. ***Example:*** *A school adds a 'My Child's Data' tab to the parent portal where a parent can download a PDF summary of data held, raise correction requests and lodge a grievance with a 15-day SLA.*
6	**Prepare for breach response** Create a written breach response plan. Establish detection, containment and notification. On any breach, notify the Board and every affected parent in the prescribed form. Maintain incident logs and corrective actions. ***Example:*** *A coaching class loses a teacher's laptop with student records. Within hours, IT revokes file access, identifies affected students, drafts a parent notification, and files a breach report to the Board.*
7	**Govern vendors and maintain records** Sign DPDP-aligned contracts with every vendor that handles student data. Maintain a Record of Processing, retention schedules, and a list of all third parties with whom data is shared. Audit annually. ***Example:*** *A school audits its vendor list and finds 14 active vendors with student data. It signs Data Processor agreements with each, sets a contract-end erasure clause, and removes three vendors that cannot meet the security baseline.*

04. Children's data: the critical focus for education

Section 9 of the DPDP Act creates a special regime for the personal data of children (anyone under 18). Educational institutes are the largest collectors of children's data in the country, which makes this the single highest area of legal exposure.

Three absolute requirements

- Verifiable parental or guardian consent must be obtained before any processing.
- No tracking or behavioural monitoring of children is permitted.
- No targeted advertising may be directed at children.

What 'verifiable' parental consent means in practice

Consent must be unambiguously linked to the actual parent or guardian of that specific child. A tick-box filled in by the student is not verifiable. Acceptable methods include: signed physical admission form with parent ID proof, OTP confirmation to the parent's registered mobile, video-KYC of the parent during enrolment, or digital signature via Digi Locker or equivalent. Siccura Consent can capture and record any of these methods and keep a time-stamped consent ledger that you can integrate into your website, parent app or admission portal.

NOTICE TO PARENTS / GUARDIANS UNDER THE DPDP ACT, 2023

[Institute Name] ("we") collects personal data of your child for the following purposes: (a) admission, academic records, attendance, marks and progress reporting; (b) fee management and statutory reporting to recognised education boards; (c) health and safety records and emergency contact; (d) transport, hostel, library and other services your child uses; (e) communication with you regarding your child's education.

Use of photographs, videos, third-party edtech tools and any other purpose not listed above will be requested separately with a fresh consent.

You have the right to access, correct, update and request erasure of your child's data, to nominate another person in case of incapacity, and to raise grievances with our Data Protection contact. You may withdraw your consent at any time; withdrawal will not affect processing already lawfully done. If your grievance is not resolved, you may approach the Data Protection Board of India.

Data Protection Contact: *Himanshu Modi — +91 90294 01855, himanshu@sumsapplication.com*

05. How SUMS ERP and the Siccura suite support each step

Four building blocks cover both layers of education data — the structured records inside your core system and the unstructured files that flow across staff laptops, drives and inboxes:

- **SUMS ERP —** the education system of record: admissions, fees, academics, transport and the parent-rights portal.
- **Siccura Discover —** finds personal data wherever it lives (Identify) and scores your risk and readiness (Audit).
- **Siccura Consent —** a dedicated consent product you can integrate into any website, app or application to capture verifiable parental consent and keep the consent ledger.
- **Siccura Regula —** protects sensitive files so the protection travels with the file, controls who can share it, and traces every action.

DPDP step	How SUMS ERP and the Siccura suite cover it
1. Discover & map	**Siccura Discover (Identify)** scans endpoints and the wider org for personal data and builds the inventory; **SUMS ERP** keeps structured student data in one place; **Siccura Regula** classifies the files it protects.
2. Notice & consent	**Siccura Consent** captures verifiable parental consent and keeps the consent ledger — integrate it into your website, parent app or admission portal; **SUMS ERP** captures consent at admission for ERP users.
3. Children's data	**Siccura Discover (Identify)** flags files containing children's data; **Siccura Consent** enforces and records verifiable parental consent; **Siccura Regula** locks children's-data files as Confidential.
4. Secure & safeguard	**Siccura Regula** keeps protection attached to each sensitive file across PCs and synced cloud folders; **Siccura Discover (Audit)** shows the protection gap and risk index as evidence; **SUMS ERP** enforces role-based access and activity logs.
5. Parent & student rights	**SUMS ERP** parent portal handle's view, correction, erasure and grievances; **Siccura Consent** holds the consent history and withdrawal records; **Siccura Regula** provides view-only sharing and a per-file trace.
6. Breach response	**Siccura Discover (Audit)** gives you readiness posture and an evidence trail; **Siccura Regula** alerts when Confidential files are shared externally; **SUMS ERP** flags unusual logins and bulk exports.
7. Govern vendors & records	**Siccura Discover (Audit)** maintains the record of processing and shows where shared data sits; **Siccura Regula** sends view-only files vendors can read but not retain; **SUMS ERP** holds the vendor directory and retention schedules.

06. Implementation checklist

Use this checklist to track your institute's DPDP readiness. Tick each item once it is implemented and documented.

- □ Appoint a Data Protection point of contact (publish name and email).
- □ Audit all places student and parent data is stored — ERP, files, drives, WhatsApp, vendor systems.
- □ Rewrite admission notice and consent forms in plain language; capture verifiable parental consent.
- □ Disable third-party trackers, analytics and ad cookies on every student-facing app and website.
- □ Classify files containing personal data as Confidential; keep protection attached and restrict sharing.
- □ Roll out parent portal access for view, correction, erasure and grievance.
- □ Document a written breach response plan; train teachers and admin staff.
- □ Sign DPDP-aligned data agreements with every vendor; set retention and erasure timelines.
- □ Conduct annual DPDP awareness training for all staff.
- □ Schedule a yearly internal audit; refresh consents and retention schedules.