



SchoolDPDPA

— Safe Data. Trusted Future. —

DPDPA COMPLIANCE TOOLKIT

FOR SCHOOLS

A Practical Guide to Protect
Student Data and Build
Parent Trust



PROTECT
Safeguard
Student Data



BUILD
Strengthen
Parent Trust



ENSURE
Meet Legal
Obligations



CREATE
A Culture of
Privacy



Author

AJESH P M

Founder & Director

SupplyFuture Technologies Private Limited (OPC)

Founder of **SchoolDPDPA**



EDITION

2026

— COMPLY TODAY. PROTECT TOMORROW. —



WHY DPDPA MATTERS FOR SCHOOLS

Schools handle a rich set of personal data every day. The Digital Personal Data Protection Act, 2023 (DPDPA) brings a new era of responsibility and accountability for every educational institution.



WHY STUDENT DATA DESERVES SPECIAL PROTECTION

Student data includes children and their families—information that can impact their safety, privacy and future opportunities. Misuse or leaks can cause harm that lasts a lifetime.



PARENTS EXPECT TRUST AND TRANSPARENCY

Today's parents want assurance that schools are careful, transparent and responsible with their data. Privacy is now a key factor in choosing and trusting a school.



STRONG GOVERNANCE BUILDS STRONGER SCHOOLS

A privacy-first culture improves efficiency, reduces risk and strengthens your reputation with parents, regulators and the community.

KEY FACTS



India's First Data Protection Law

DPDPA, 2023 sets the foundation for data privacy and digital trust in India.



Personal Data is a Responsibility

Schools are Data Fiduciaries and must follow lawful, fair and transparent practices.



Children Need Higher Protection

The Act recognizes the need for additional safeguards for children's data.



Non-Compliance Can Be Costly

Significant financial penalties and reputational damage can impact your school.

WHY ACT NOW?



REDUCE RISK

Minimize the chance of data breaches, complaints and legal penalties.



EARN TRUST

Build confidence with parents, students and your community.



IMPROVE OPERATIONS

Better data governance leads to efficient processes and better decision-making.



STAY AHEAD

Prepare today and create a future-ready, privacy-first institution.



Protecting data is not just about compliance. It is about protecting futures and building lifelong trust.



UNDERSTANDING DPDPA FOR SCHOOLS

The Digital Personal Data Protection Act, 2023 (DPDPA) is India’s landmark law to protect the personal data of individuals in the digital world.

For schools, it sets clear expectations for how student, parent and staff data must be collected, used, stored and shared.



In simple terms:

DPDPA gives individuals (and in the case of children, their parents/guardians) control over their personal data and places responsibilities on organisations that handle it.

CORE PRINCIPLES OF DPDPA



Lawful & Fair
Collect data only for lawful, clear and legitimate purposes.



Purpose Limitation
Use data only for the purpose it was collected.



Data Minimisation
Collect only the data that is necessary.



Accuracy
Keep data accurate, complete and up to date.



Storage Limitation
Retain data only as long as required.



Security Safeguards
Protect data with appropriate technical and organisational measures.



Accountability
Be accountable and demonstrate compliance with the Act.

KEY OBLIGATIONS FOR SCHOOLS (AS DATA FIDUCIARIES)



Notice & Transparency

Inform parents/students about what data is collected, why, how it is used, shared and how long it is retained.



Consent Management

Obtain valid consent from parents/guardians (and from students where applicable) before collecting personal data.



Rights of Individuals

Respect data principal rights such as access, correction, erasure and withdrawal of consent.



Data Security

Implement safeguards to prevent data breaches, leaks, unauthorised access or misuse.



Breach Notification

Report personal data breaches to the Data Protection Board of India and affected individuals.



Responsible Governance

Ensure policies, training, contracts and vendor management are in place.

RIGHTS OF PARENTS / GUARDIANS AND STUDENTS



Right to Access
Know what data is held and how it is used.



Right to Correction
Correct inaccurate or incomplete data.



Right to Erasure
Request deletion of data when no longer needed.



Right to Withdraw Consent
Withdraw consent and stop further processing.



Right to Grievance Redressal
Lodge complaints and seek timely resolution.



DPDPA is not just a legal requirement.
It is an opportunity to build a culture of privacy, respect and trust in your school.



WHAT PERSONAL DATA SCHOOLS HANDLE

Schools collect and process a wide range of personal data in the course of their educational and administrative activities.

Understanding what data you handle is the first step to protecting it.



Remember

Any information that can identify a person, directly or indirectly, is personal data under DPDPA.



- ### 1. STUDENT DATA
- Name, date of birth, gender
 - Address and contact details
 - Admission and academic records
 - Attendance, assignments, exam results
 - Behavioural and disciplinary records
 - ID cards, roll numbers
 - Photographs and videos



- ### 2. PARENT / GUARDIAN DATA
- Name and contact details
 - Relationship with student
 - Address and communication history
 - Identification proof (if collected)
 - Payment and fee-related information
 - Consent and preference records



- ### 3. STAFF DATA
- Personal and contact details
 - Qualifications and experience
 - Employment records and payroll data
 - Performance and appraisal records
 - Leave and attendance data
 - Identification documents



- ### 4. FINANCIAL DATA
- Fee payments and refunds
 - Bank account and transaction details
 - Scholarship and concession records
 - Invoices and receipts
 - Payroll and staff compensation data



- ### 5. IMAGE & AUDIO / VIDEO DATA
- CCTV footage
 - Event photographs and videos
 - Online class recordings
 - School activities and competitions
 - Biometric data (if used)



- ### 6. HEALTH & SAFETY DATA
- Medical history and health conditions
 - Immunisation records
 - Emergency contact information
 - Accident and incident reports
 - Counselling and well-being records



- ### 7. TRANSPORT DATA
- Route and pickup/drop details
 - Transport charges and payments
 - Driver and attendant information
 - GPS / tracking data (if used)



- ### 8. DIGITAL & ONLINE DATA
- Email and communication records
 - LMS / portal login and usage data
 - IP addresses and device information
 - Cookies and website analytics data
 - Online form submissions

OTHER EXAMPLES



- Library usage
- Hostel / accommodation details
- Alumni records
- Event registrations
- Visitor log and ID proofs
- Vendor / service provider data
- Donations and sponsorships
- Social media interactions



Not all data is equally sensitive, but all data deserves protection.

Know what you collect. Limit what you need. Protect what you have.



DATA LIFE CYCLE & SCHOOL RESPONSIBILITIES

Personal data moves through a life cycle. At each stage, schools must follow lawful, fair and secure practices. Strong controls at every step reduce risk and build trust.



LAWFUL & FAIR COLLECTION

Collect data only for clear, legitimate and lawful purposes with appropriate consent and transparency.



PURPOSE LIMITATION

Use data only for the purpose it was collected. Do not use it for unrelated activities.



SECURE STORAGE

Store data securely with appropriate technical and organisational safeguards to prevent unauthorised access, loss or misuse.



USE & DISCLOSURE

Share data only when necessary and with authorised parties such as government authorities, service providers or as required by law.



RETENTION & DELETION

Retain data only for as long as needed to fulfil the purpose. Securely delete or anonymise it when no longer required.



ACCOUNTABILITY & REVIEW

Regularly review policies, processes and systems. Maintain records and demonstrate compliance with DPDPA.

THE DATA LIFE CYCLE



1 COLLECT

Collect only necessary data with valid consent and transparency.



2 USE

Use data only for the stated purpose and in accordance with the law.



3 STORE

Store data securely and protect it from loss, unauthorised access or misuse.



4 SHARE

Share data only with authorised recipients and under legal obligations or with consent.



5 RETAIN

Retain data only for the period necessary to achieve the purpose.



6 DELETE / ANONYMIZE

Securely delete or anonymise data when it is no longer needed or when requested.

BEST PRACTICES FOR SCHOOLS



PRIVACY BY DESIGN

Build privacy into systems, processes and school culture from the start.



TRAIN & AWARE

Train staff regularly on data protection policies, roles and responsibilities.



DOCUMENT & RECORD

Maintain records of consent, policies, data processing activities and data sharing.



LEAST PRIVILEGE

Give access to data only to those who need it to do their assigned work.



TECHNOLOGY SAFEGUARDS

Use strong passwords, encryption, backups and secure software configurations.



MONITOR & IMPROVE

Audit regularly, identify gaps and continuously improve your practices.



Data is an asset. With the right controls, it becomes a source of trust and better outcomes for students and the school community.





CONSENT

THE FOUNDATION OF TRUST

DPDPA places consent at the heart of lawful data processing. For schools, this means being clear, transparent and respectful about how personal data is collected and used.

Good consent practices build confidence with parents, students and the wider community.

TYPES OF CONSENT SCHOOLS MAY NEED

- | | |
|---|--|
|  Collecting student data at admission and during the school year |  Health, counselling or other sensitive information |
|  Using photographs, videos or testimonials |  International trips, events and activities |
|  Sharing information with third parties (vendors, service providers) |  Use of digital tools, apps or online platforms |
|  Marketing, newsletters or promotional activities |  Scholarships, financial assistance and concessions |

WHAT IS VALID CONSENT?

- **Freely Given**
No pressure or coercion; a genuine choice.
- **Informed**
Clear information about what data is collected, why, how and for how long.
- **Specific**
Given for specific purposes, not for broad or unclear reasons.
- **Unambiguous**
An explicit action (written, digital or ticked choice) showing agreement.
- **Revocable**
Individuals can withdraw consent at any time, as easy as giving it.

BEST PRACTICES FOR OBTAINING CONSENT

- | | | | | | |
|---|---|---|---|--|--|
|  Be Transparent
Use simple language that parents and students can easily understand. |  Provide Options
Offer clear choices (opt-in) and avoid bundled or forced consent. |  Document Properly
Record when, how and for what purpose consent was obtained. |  Keep Updated
Review and renew consent when purposes change. |  Easy Withdrawal
Make it simple for individuals to withdraw consent and respect their decision. |  Student-Appropriate
Take age-appropriate consent and explain in a way children can understand. |
|---|---|---|---|--|--|

PRACTICAL EXAMPLE



Before using student photos on the school website, obtain explicit consent from parents/guardians. Provide details of where it will be used, for how long, and the option to withdraw at any time.

SCHOOLS SHOULD ENSURE



- ✓ Consent forms are easy to access and understand.
- ✓ Digital consent platform is secure and auditable.
- ✓ Records are stored securely and are always up to date.
- ✓ Staff know when consent is required and how to obtain it.

“

Consent is not just a form. It is a relationship built on respect, clarity and the right to choose.





DATA SECURITY SAFEGUARDS PROTECT WHAT MATTERS MOST

DPDPA requires schools to implement appropriate technical and organisational measures to protect personal data from breaches, loss, misuse and unauthorised access.

Strong safeguards not only ensure compliance but also build trust with parents, students and staff.

THE IMPACT OF POOR DATA SECURITY



Data breaches can expose sensitive information and cause harm.



Non-compliance can lead to heavy financial penalties and legal consequences.



Loss of trust can damage reputation and affects student enrolment.



Operational disruption can impact teaching, learning and safety.

KEY TECHNICAL & ORGANISATIONAL SAFEGUARDS



Access Control

Restrict access to personal data on a need-to-know basis. Use strong passwords and multi-factor authentication.



Data Encryption

Encrypt data in transit and at rest, especially for sensitive information.



Secure Storage

Store data in secure systems and trusted cloud services with regular backups.



System Protection

Use firewalls, anti-malware, regular patches and secure configurations to protect systems.



Staff Awareness & Training

Train staff regularly on data protection policies, phishing risks and secure handling of data.



Policies & Procedures

Adopt clear data protection policies, incident response plans and vendor management processes.



Monitoring & Audits

Monitor systems, review access logs and conduct regular audits to detect and address risks.

SCHOOL DATA SECURITY CHECKLIST



Strong password policy and MFA implemented



Access granted only on need-to-know basis



Data encrypted in transit and at rest



Regular backups tested and secured



Staff trained on data protection practices



Policies and contracts in place



Incident response plan ready and communicated



Regular reviews and audits conducted



REMEMBER

There is no 100% security. The goal is to reduce risk, respond quickly and continuously improve.



GOOD TO KNOW

Data security is a shared responsibility. Every staff member plays a part.



Protecting data is protecting people.
Strong security today, safer students tomorrow.





RIGHTS OF INDIVIDUALS (STUDENTS & PARENTS)

DPDPA empowers individuals with control over their personal data. Schools must respect these rights and respond in a transparent and timely manner.

These rights apply to students, parents/guardians and, where relevant, staff members.

KEY RIGHTS UNDER DPDPA



1. Right to Access

Know what personal data is held about you and how it is being used.



2. Right to Correction

Request correction of inaccurate, incomplete or outdated personal data.



3. Right to Erasure

Request deletion of personal data when it is no longer necessary for the purpose.



4. Right to Withdraw Consent

Withdraw consent for the processing of your data and stop further processing.



5. Right to Grievance Redressal

Lodge a complaint with the Data Fiduciary and seek timely resolution.



6. Right to Nominate

Nominate a person to exercise your rights in the event of incapacity or death.

HOW SCHOOLS SHOULD HANDLE RIGHTS REQUESTS



1. Receive

Accept requests in writing or through designated digital channels.



2. Verify

Verify the identity of the requester to prevent unauthorised access.



3. Assess

Review the request and determine applicability and feasibility.



4. Act

Take necessary action (provide access, correct, erase, stop processing or withdraw consent).



5. Communicate

Respond within the prescribed timelines with clear information on the action taken.



6. Record

Maintain records of all requests, actions and responses for accountability.

RESPONSE TIMELINES (AS PER DPDPA)



Within 15 Days

Respond to most rights requests within 15 days of receipt.



Up to 30 Days

May extend by up to 15 additional days in cases of complexity. Inform the requester within the initial 15 days.



In Case of Denial

If a request is denied (in whole or in part), provide clear reasons and information on available grievance redressal.

SCHOOLS MAY DENY A REQUEST IF:



Fulfilling the request would undermine the sovereignty and integrity of India, the security of the State, public order or prevention of offences.



The request is frivolous, vexatious or repetitive.



Compliance would breach any other law for the time being in force.



The data is necessary for the performance of a legal obligation or for a task in the public interest.



The data is no longer in the possession of the school.

“

Respecting individual rights builds trust and strengthens relationships.
Empowered individuals create stronger school communities.





ROLES & RESPONSIBILITIES

BUILDING A CULTURE OF COMPLIANCE

DPDPA compliance is a shared responsibility. Every individual in the school community has a role to play in protecting personal data and maintaining trust.

Clear roles, defined responsibilities and accountability ensure compliance becomes a way of working.

PILLARS OF ACCOUNTABILITY



CLEAR ROLES
Define responsibilities for everyone involved.



STRONG POLICIES
Documented policies guide daily actions and decisions.



REGULAR TRAINING
Build awareness and keep skills and knowledge current.



CONTINUOUS REVIEW
Monitor, audit and improve processes regularly.

WHO DOES WHAT?



SCHOOL MANAGEMENT
Sets the tone, approves policies, allocates resources and ensures accountability.



DATA FIDUCIARY
Oversees compliance, manages risks, handles rights requests and acts as the point of contact.



STAFF MEMBERS
Handle personal data responsibly, follow policies and report incidents or concerns.



PARENTS / GUARDIANS
Provide accurate information, give consent and stay informed about their rights.



STUDENTS
Understand data privacy, respect others' information and report misuse.



THIRD-PARTY VENDORS
Process data only as authorised, follow contractual obligations and maintain appropriate safeguards.

DO'S



Collect only the personal data you need for clear and lawful purposes.



Inform individuals about why data is collected, how it will be used and for how long.



Store data securely and restrict access to authorised people only.



Retain data only for as long as necessary and delete/anonymise when no longer needed.



Respond to rights requests within the timelines prescribed under DPDPA.



Train staff and students regularly on data protection and privacy.

DON'TS



Do not collect excessive or unnecessary personal data.



Do not share personal data without a lawful basis or consent.



Do not use personal data for marketing or other unrelated purposes.



Do not store data on personal devices or unsecured platforms.



Do not ignore data breach incidents or delay reporting.



Do not alter or delete data to avoid compliance obligations.



Compliance is not just about avoiding penalties.
It is about building trust, protecting individuals and strengthening your school.





DATA BREACH

RESPONSE & INCIDENT

MANAGEMENT

BE PREPARED, ACT FAST,

REDUCE IMPACT

A data breach can happen despite best efforts. What matters most is how quickly and effectively you respond.

A clear incident response plan helps reduce harm, meet legal obligations and maintain trust.

WHAT IS A DATA BREACH?



A data breach is any unauthorised access, use, disclosure, alteration, loss or destruction of personal data that compromises the confidentiality, integrity or availability of the data.

EXAMPLES



Hacking or malware attack



Loss or theft of devices or documents



Unauthorised access by staff or third parties



Cloud misconfiguration or data leak



Accidental disclosure of personal data

INCIDENT RESPONSE: 6 KEY STEPS

1



IDENTIFY

Detect and confirm the incident. Assess the nature and scope of the breach.

2



CONTAIN

Take immediate steps to stop the breach and secure systems and data.

3



ASSESS

Evaluate the impact, data involved and who may be affected.

4



NOTIFY

Notify the Data Fiduciary and affected individuals within the timelines prescribed under DPDPA.

5



RESPOND & RECOVER

Investigate the cause, mitigate further risk and restore systems and services securely.

6



REVIEW & IMPROVE

Document the incident, review controls and improve policies, processes and training.

NOTIFICATION TIMELINES



TO THE DATA FIDUCIARY

As soon as practicable and in any case within 72 hours of becoming aware of the breach.



TO AFFECTED INDIVIDUALS

As soon as practicable and in any case within a reasonable time after assessing the risk.



INFORMATION TO INCLUDE

- Nature of the breach
- Categories and number of individuals affected
- Likely consequences
- Measures taken or proposed to be taken
- Contact details for further information

PREPARE IN ADVANCE



PLAN

Create and document an incident response plan.



TEAM

Assign roles and responsibilities to a response team.



TRAIN

Train staff regularly on identifying and reporting incidents.



TEST

Test your plan and backup systems periodically.



UPDATE

Review and update the plan as threats and systems evolve.

REPORT IT!



If you suspect a data breach or security incident, report it immediately to:



DATA FIDUCIARY OFFICER (DFO)

✉ dfo@schoolname.edu.in

☎ +91 12345 67890

WHEN IN DOUBT, REPORT.



Early reporting can prevent greater harm and protect our school community.



Preparation is your best protection.
Responding quickly and transparently is the mark of a responsible school.





ABOUT THE AUTHOR



Ajesh P M

Founder & Director
SupplyFuture Technologies
Private Limited (OPC)



ABOUT THE AUTHOR

Ajesh P M is the Founder & Director of SupplyFuture Technologies Private Limited (OPC). He specializes in data privacy, cybersecurity, digital transformation and compliance solutions for educational institutions. Through SchoolDPDPA, he helps schools understand the Digital Personal Data Protection Act, 2023 and implement practical, school-friendly privacy frameworks that protect student information, strengthen governance and build parent trust.



ABOUT SCHOOLDPDPA

SchoolDPDPA is an initiative focused on helping schools implement practical and sustainable data protection practices. Our services include DPDPA readiness assessments, policy development, parent consent frameworks, staff awareness training, cybersecurity guidance and ongoing compliance support for schools across India.



OUR MISSION

“ Helping every school become privacy-first, compliant and trusted.



CONTACT



Website
www.schooldpdpa.com



Email
contact@schooldpdpa.com



Phone
+91 80750 51679



Safe Data. Trusted Future.





SchoolDPDPA

—— Safe Data. Trusted Future. ——