# KSHAMTALAYA FOUNDATION

## DATA PROTECTION POLICY

*Aligned with the Digital Personal Data Protection Act 2023 and DPDP Rules 2025*

CIN: U74999RJ2016NPL055597 | Incorporated 27 July 2016 | Section 8 Company | Companies Act 2013

14, Mateshwari Colony, Opp.Sai Temple, Bedla Road, Badgaon, Udaipur, Rajasthan

| Field | Details | Field | Details |
|---|---|---|---|
| **Version** | 2.0 | **Effective Date** | 1 June 2026 |
| **Applicable to** | All staff, consultants, interns, volunteers, partners | **Review Cycle** | Annual, or earlier if law changes |
| **Sign-off Authority** | Board Chair | **DPO Contact** | abhishek@kshamtalaya.org |

## 1. About Kshamtalaya Foundation

Kshamtalaya is a Section 8 Non-Governmental Organisation working across Rajasthan, Delhi, and Bihar. Our work focuses on Learning, Wellbeing, and Governance, and our goal is to transform the quality of public education at the last mile.

The people we work with include children (Grades 1-12), teachers, parents, PRI members, SMC members, education functionaries, youth, partner organisations, and our own team.

This policy covers how we collect, use, store, share, and erase personal data of:

- Our partners and stakeholders, including children and their families
- Our team members such as employees, consultants, volunteers, interns, and contractual staff
- Partner organisations we work with

## 2. The Law We Are Working Under

India's Digital Personal Data Protection Act 2023 (DPDP Act) came into full effect with the notification of the DPDP Rules 2025 on 14 November 2025. This is now the primary law governing how organisations like ours handle personal data.

As an organisation that collects and processes personal data of children, teachers, community members, and our own staff, we are a Data Fiduciary under the Act. That means we are legally responsible for how that data is handled, from collection to erasure.

This policy is our commitment to meeting those responsibilities. Where the Act does not specify detail, we follow the General Data Protection Regulation (GDPR) as a reference for best practice.

### 2.1 Key Terms

We use the following terms throughout this policy, drawn directly from the DPDP Act 2023:

| Term | What it means |
|---|---|
| **Personal Data** | Any data about a person who can be identified from it. |

| | |
|---|---|
| **Data Principal** | The person the data belongs to. In the case of a child, this includes the parent or guardian. |
| **Data Fiduciary** | The organisation that decides why and how personal data is processed. That is us. |
| **Data Processor** | Any person or organisation that processes data on our behalf. For example, a technology platform or a data analysis vendor. |
| **Consent** | A freely given, specific, informed, and unambiguous agreement to data being collected and used. |
| **Personal Data Breach** | Any unauthorised access, sharing, loss, or destruction of personal data. |
| **Child** | Anyone under 18 years of age. |
| **Data Protection Board** | The Data Protection Board of India, which oversees compliance with the Act and handles complaints. |

## 3. Our Principles for Handling Personal Data

We are aware that the people whose data we hold, particularly children, may not always fully understand how their data could be used or what their rights are. That makes it our responsibility to handle it carefully and honestly.

We are committed to building a safe environment for everyone connected with the organisation. In practice, this means:

- We collect data only with proper consent. For children, we take verifiable consent from the parent or guardian before collecting anything.
- We use data only for what we said we would use it for. Nothing more.
- We keep data accurate, and we update or erase it when it is no longer correct or needed.
- We protect data against accidental or unauthorised access, disclosure, or destruction.
- We are accountable for these commitments, to the law and the communities we work with.

All staff are expected to follow these principles when handling personal data. Any suggestions for how we can do better should be sent to the DPO at the email address listed in Section 17.

## 4. What Data We Collect and Why

We collect personal data to monitor and evaluate programme delivery, understand who we are working with, and continually improve the services we provide. Below is a breakdown of the data we collect from each group of stakeholders.

| Who | What we collect | Why we collect it / Legal basis |
|---|---|---|
| Children (Grades 1-12) | Name, age, gender, parents' name, parents' education and occupation, school serial number, attendance, learning levels | Programme monitoring and evaluation. We take verifiable parental or guardian consent before collecting any data about children (Section 9, Rule 10, DPDP Act). |
| Teachers | Name, gender, years of experience, subjects, designation, school name and UDISE code | Programme delivery and teacher capacity tracking. Based on consent and legitimate interest. |

| | | |
|---|---|---|
| Parents, PRI members, SMC members, community | Name, contact details, role, records of engagement with the programme | Community governance and outreach tracking. Based on consent. |
| Employees and contractual staff | Name, contact details, employment records, bank details (payroll), tax identification, performance records | HR and payroll management. Required by our employment contract and applicable law. |
| Consultants, interns, volunteers | Name, contact details, engagement terms, outputs | Engagement management. Based on contractual necessity and consent. |
| Partner organisations | Contact details of representatives, MoU terms, project-related data | Partnership management. Based on contractual necessity and legitimate interest. |

We also share responsibility with our funding partners for data collected as part of jointly run projects. Our MoUs with partners set out each party's obligations around data collection, storage, and protection.

## 5. How We Take Consent

Consent is the primary basis on which we collect personal data, especially for our programme stakeholders. For consent to be valid, it must be:

- Freely given: no one should feel pressured to share their data
- Specific: we are clear about what data we are collecting and for what purpose
- Informed: we explain in plain language what will happen to the data
- Unambiguous: silence or inaction is not consent; we need an active agreement, whether that is a signature, a verbal confirmation recorded in writing, or a tick-box

### 5.1 Consent for Children's Data

Because we work primarily with children, this is the most important part of our consent process. The DPDP Act requires us to obtain verifiable consent from a parent or lawful guardian before collecting any personal data about a child.

In practice, this is how we do it:

- We use a consent form written in a language the parent or guardian can understand
- We verify who the consenting adult is. This can be through a government-issued ID, school admission records, or DigiLocker-based verification
- We keep a record of every consent obtained, including how we verified it, for a minimum of 7 years
- We never track, monitor, profile, or target children for any purpose beyond what is stated in the consent
- We never use children's data for any purpose other than the programme it was collected for

### 5.2 Withdrawing Consent

Anyone whose data we hold can withdraw their consent at any time. When they do:

- We stop processing their data within 30 days of the withdrawal
- We give them at least 48 hours' notice before we erase their data, so they can raise any concerns
- If we are legally required to retain some data even after consent is withdrawn such as for tax records, we will explain this clearly

## 6. What We Tell People Before Collecting Their Data

Before we collect any personal data, we make sure the person knows:

- What data we are collecting
- Why we are collecting it and how we will use it
- Who else might see it or receive it
- How long we will keep it
- What rights they have and how to exercise them
- How to withdraw consent if they change their mind

We make this information available in a language the person can actually understand. For children's data, we make sure this information reaches the parent or guardian.

## 7. How We Store and Manage Data

### 7.1 General Approach

Our data management approach is built around limiting who can access data to only the people who need it, and keeping all data on platforms we control and can secure.

- Every staff member signs a contract that includes a data confidentiality clause
- Volunteers sign a non-disclosure agreement before accessing any personal data
- Data is stored only on our authorised platforms: our G Suite (Google Workspace on the Kshamtalaya domain), CommCare, and Moodle. Storing organisational data on personal Gmail accounts is not permitted
- Access to data is limited based on role. People can only see the data relevant to their work
- We back up all data on a weekly basis, with the same access controls as primary data
- All devices used to access our data must have up-to-date software and security patches installed

> **Important:** All staff using Google Workspace must access it through their Kshamtalaya domain account (e.g. @kshamtalaya.org), not a personal Gmail account. Domain-level security settings apply only to domain accounts. Personal Gmail is outside our administrative control and should not be used for storing or sharing programme data.

### 7.2 Platforms We Use

| Platform | What we use it for | Controls in place |
|---|---|---|
| G Suite (Google Workspace) | Data collection via Google Forms, storage via Google Drive, analysis via Sheets and Data Studio | Access restricted to Kshamtalaya domain accounts only; folders are permission-controlled; personal Gmail is not authorised |
| CommCare | Field data collection and stakeholder tracking | Installed only on authorised devices; password-protected; role-based access; field users see only their assigned data |
| Moodle | Learning programme delivery and participant progress tracking | Consent taken at sign-up; access limited to relevant programme staff |

## 8. What We Use Data For and How Long We Keep It

The table below sets out each processing activity, the data it involves, why we do it, and how long we keep it.

| What we do with it | Data involved | Basis | How long we keep it |
|---|---|---|---|
| Programme monitoring and evaluation | Attendance, learning levels, intervention records of children and teachers | Verifiable parental consent (children); consent (others) | Duration of programme, plus 5 years for impact tracking |
| Impact reporting to funders | Aggregated, anonymised programme data; anonymised case studies | Legitimate interest; specific consent for case studies | Duration of funding agreement, plus 7 years |
| HR and staff management | Employment records, payroll data, tax details, performance records | Contractual necessity; legal obligation | Duration of employment, plus 7 years (Income Tax Act) |
| Stakeholder and partner communications | Contact details of partners, funders, stakeholders | Consent; legitimate interest | Duration of active relationship, plus 2 years |
| Legal and compliance records | Contracts, MoUs, statutory filings | Legal obligation | Minimum 8 years from date of record (Companies Act 2013) |
| Security and access logs | Device and system access logs | Legitimate interest | 12 months, reviewed annually |

Once the relevant retention period ends, we erase or permanently anonymise the data. Where we plan to erase someone's data, we give them at least 48 hours' notice beforehand.

## 9. Who We Share Data With

We do not share individual personal data with third-party organisations unless one of the following applies:

- The person has given explicit consent to that specific sharing
- We are required to share it under a contract with a partner or funder, and a Data Processing Agreement is in place
- We are legally required to share it with an authority or regulator

### 9.1 Funding Partners

Where we share data with a funder or partner as part of a project, the MoU or Data Processing Agreement between us sets out what data is shared, for what purpose, what security standards apply, and that the partner cannot share it further without our written agreement.

### 9.2 Aggregated Data

We share overall programme data with funders and in public communications such as total attendance figures for a year group, or the average learning levels of children in a cohort. This data is always anonymised. We do not name individuals in these communications.

**Commented [1]:** Action needed: A Data Processing Agreement (DPA) aligned with the DPDP Act 2023 must be in place with any partner that receives personal data from us, including Educate for Life. The DPA should cover the specific data categories shared, the permitted uses, security obligations, and the process for handling data breaches and Data Principal rights requests. recommend developing a standard DPA template for our MoU toolkit.

**Commented [2R1]:** need to add this

### 9.3 Case Studies and Stories

If we want to share a quote, case study, or personal story about a programme participant, we always get explicit written consent first. For children, that consent comes from the parent or guardian. The consent form documents exactly what will be shared, where, and for how long.

We make it clear to people that participation in the programme is not conditional on sharing their story. No one loses access to our services by saying no.

Where names or other identifying details are not essential to the story, we use initials or a pseudonym.

### 9.4 Photography and Images

Any photos or videos involving children or beneficiaries are taken and shared in line with our Child Protection Policy. Where identifying consent has not been given, we blur or obscure faces before sharing images on social media or in publications.

## 10. How We Keep Data Secure

Keeping personal data safe is everyone's responsibility, not just the DPO's. The Act requires us to put in place reasonable security safeguards, and here is what that looks like for us.

### 10.1 Technical Measures

- Data in transit and at rest is encrypted wherever our authorised platforms support it
- All data systems require unique login credentials and role-based permissions
- All devices used to access our data must be password-protected
- Operating systems and applications must be kept up to date to address security vulnerabilities
- When a staff member changes role or leaves, their access is revoked immediately

### 10.2 Administrative Measures

- Every staff member and volunteer signs a confidentiality agreement before accessing personal data
- All staff receive a data protection briefing when they join and a refresher at least once a year
- The DPO oversees data protection compliance across the organisation
- Data protection is part of how we evaluate vendors and technology partners before working with them

## 11. What We Do If There Is a Data Breach

A data breach is any incident where personal data is accessed, shared, lost, or destroyed without authorisation. This includes:

- Unauthorised disclosure of personal data
- Loss or theft of a device or physical record containing personal data
- Unauthorised access to our data systems, including via hacking
- Accidentally sending personal data to the wrong person
- Any destruction or loss of data that prevents us from accessing it

### 11.1 Reporting a Breach

If any staff member, volunteer, consultant, or partner discovers or suspects a data breach, they must report it to the DPO within 6 hours of becoming aware. Do not try to handle it independently.

The report should include:

- When the breach was discovered
- What happened, as far as is known
- Which categories of data and how many people are affected
- What action has already been taken

### 11.2 What We Do Next

Once a breach is reported, the DPO will:

- Contain the breach and preserve evidence immediately
- Notify affected Data Principals without delay, in plain language, explaining what happened and what they should do
- Report the breach to the Data Protection Board of India within 72 hours of becoming aware of it, as required under Rule 7 of the DPDP Rules 2025
- Submit a detailed follow-up report to the Board within 72 hours (or within any extended period the Board approves)
- Complete a full incident review, including root cause analysis and remedial steps, within 14 days of resolution

> **Penalty note: Failure to notify the Data Protection Board of a breach can attract a penalty of up to ₹200 crore per incident. Failure to maintain adequate security safeguards can attract penalties of up to ₹250 crore (DPDP Act 2023).**

## 12. Rights of the People Whose Data We Hold

Everyone whose personal data we process has rights under the DPDP Act 2023. We are committed to making it easy for people to exercise these rights.

| Right | What it means | How to use it |
|---|---|---|
| Right to be informed | You have the right to know what data we collect about you, why, and how we use it, before we collect it. | Covered in the privacy notice at the point of data collection. |
| Right of access | You can ask us what personal data we hold about you. This is free of charge. | Send a Subject Access Request (SAR) to the DPO. |
| Right to correction | If we hold inaccurate or incomplete data about you, you can ask us to correct it. | Write to the DPO. |
| Right to erasure | You can ask us to erase your data. We may decline if we are legally required to keep it, or if it is needed for a legal claim. | Write to the DPO. |
| Right to grievance redressal | If you have a complaint about how we are handling your data, you can raise it with us. We will respond within 30 days. If you are not satisfied, you can escalate to the Data Protection Board of India. | Contact the DPO. |
| Right to nominate | You can nominate someone to exercise your rights on your behalf if you are unable to do so yourself. | Submit a written nomination to the DPO. |
| Right to withdraw consent | You can withdraw your consent at any time. This does not affect anything we have already done lawfully on the basis of that consent. | Contact the DPO or your programme manager in writing. |

We will respond to all rights requests within 30 calendar days. If a request is complex, we may extend this by a further 30 days and will tell you if we do.

## 13. Subject Access Requests

When a staff member receives a request from someone about their personal data rights:

- Do not respond directly or share any information. This is important.
- Forward the request to the DPO immediately.
- The DPO will acknowledge the request within 5 working days and provide a full response within 30 calendar days.
- If we need to verify the person's identity before responding, the DPO will ask for this in the acknowledgement.
- There is no charge for this.

## 14. Requests from Authorities or Third Parties

If we receive a request for personal data from a government authority, regulator, or any external organisation, the staff member who receives it must:

- Not share any data with the requesting party
- Forward the request to the DPO immediately

The DPO will assess whether the request is lawful and, if needed, consult legal counsel before deciding whether to comply.

## 15. Working with Third-Party Platforms and Vendors

Where we use a third-party platform or vendor to process personal data on our behalf such as a data analysis service or a technology provider, the programme manager responsible for that relationship must ensure:

- A written contract or Data Processing Agreement is in place before any data is shared
- The contract requires the vendor to implement security measures appropriate to the risk
- The contract restricts the vendor from using the data for any purpose other than the one we have specified

Where we are processing data jointly with a partner organisation, our contract with them must clearly set out each party's responsibilities for that data.

## 16. Sending Data Outside India

The DPDP Act allows personal data to be transferred outside India, but the government can restrict transfers to certain countries. Before transferring any personal data internationally, we need to check:

- That the destination country has not been restricted by the Central Government under the Act
- That a written agreement is in place with the receiving organisation, requiring them to protect the data to the same standard as the Act requires
- That the DPO has reviewed and approved the transfer

Any new process that may involve sending personal data outside India should be discussed with the DPO before it starts.

> **Where government guidance has not yet been issued,** we use the GDPR framework including adequacy decisions and Standard Contractual Clauses, as a reference for assessing whether the receiving country or organisation provides adequate protection.

## 17. Our Data Protection Officer

The DPDP Rules 2025 require us to designate a person responsible for data protection and to publish their contact details. Our DPO is the first point of contact for any data protection question, request, or complaint.

| Role | Details |
|---|---|
| Name | Abhishek Kumar Tiwari |
| Designation | Data Protection Officer (DPO) |
| Organisation | Kshamtalaya Foundation |
| Email | abhishek@kshamtalaya.org |
| Postal address | 14, Mateshwari Colony, Opp. Sai Temple, Bedla Road, Bedla, Udaipur (Raj.) |
| Response time for grievances | 30 calendar days from receipt of complaint |

## 18. Training

Everyone who handles personal data as part of their work at Kshamtalaya Foundation must:

- Complete a data protection orientation when they join
- Attend a refresher at least once every 12 months
- Sign the Policy Declaration form to confirm they have read and understood this policy

The DPO is responsible for keeping training materials up to date and making sure changes to the law or this policy are communicated to all relevant staff.

## 19. If This Policy Is Breached

If you suspect this policy has been breached in any way, report it to the DPO immediately through the same channel as a data breach (Section 11.1).

Depending on how serious the breach is:

- The staff member responsible may face disciplinary action, up to and including termination
- We may be required to report the breach to the Data Protection Board of India
- We may be subject to penalties under the Act

## 20. Reviewing This Policy

We review this policy at least once a year. We will also review it earlier if:

- The DPDP Act or Rules change
- A significant data breach or near-miss occurs
- Our data processing activities change substantially

Any changes need approval from the Board of Directors. The DPO is responsible for keeping this policy current and communicating updates to the team.

## Annexure A: Definitions

The following terms are drawn from the Digital Personal Data Protection Act 2023 (Act No. 22 of 2023):

| Term | Definition (from the DPDP Act 2023) |
|---|---|
| **Personal Data** | Any data about an individual who is identifiable by or in relation to such data. (Section 2(t)) |
| **Data Principal** | The individual to whom the personal data relates. In the case of a child or a person with disability, includes the parent or lawful guardian. (Section 2(j)) |
| **Data Fiduciary** | Any person who alone or in combination with others determines the purpose and means of processing personal data. (Section 2(i)) |
| **Data Processor** | Any person who processes personal data on behalf of a Data Fiduciary. (Section 2(k)) |
| **Processing** | A wholly or partly automated operation on digital personal data, including collection, recording, storage, use, disclosure, erasure, or destruction. (Section 2(x)) |
| **Consent** | Free, specific, informed, unconditional, and unambiguous consent given through a clear affirmative action. (Section 6) |
| **Personal Data Breach** | Any unauthorised processing or accidental disclosure, acquisition, sharing, use, alteration, destruction, or loss of access to personal data that compromises its confidentiality, integrity, or availability. (Section 2(u)) |
| **Child** | An individual who has not completed 18 years of age. (Section 2(d)) |
| **Significant Data Fiduciary** | A Data Fiduciary designated as such by the Central Government based on volume and sensitivity of data processed, risk to Data Principals, or national security considerations. (Section 10) |
| **Data Protection Board** | The Data Protection Board of India, established under Section 18, with jurisdiction over complaints and enforcement. |

## Annexure B: Examples of Personal Data We Collect

Below are examples of the personal data we collect from our programme stakeholders, as referenced throughout this policy.

**Children (General) -** Name, age, gender, parents' name, parents' educational qualification and work status, school serial number

**Teachers -** Name, gender, years of experience, subjects taught, designation, school name and DISE code

**Outcome data -** Attendance of children, learning levels

**School information -** School name, staff details, DISE code

**Intervention data -** Records of classroom interventions, teacher engagement sessions, community participation in school processes

## Annexure C: References

This policy draws on the following sources:

1. Digital Personal Data Protection Act 2023 (Act No. 22 of 2023)
2. Digital Personal Data Protection Rules 2025 (notified 14 November 2025, G.S.R. 843(E))
3. General Data Protection Regulation (EU) 2016/679 (GDPR) - used as a best-practice reference where the DPDP Act does not specify detail
4. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (SPDI Rules) under the IT Act 2000
5. Data Protection Policy of CSEI
6. EFL Data Protection Policy

## Sign-Off and Version History

| Name | Designation | Signature | Date |
|---|---|---|---|
| Anjali Gupte | Board Chair / Authorised Signatory | | |
| Abhishek Kumar Tiwari | Data Protection Officer | | |

| Version | Date | Revised by | Summary of changes |
|---|---|---|---|
| 1.0 | 2023 | Kshamtalaya Foundation | Original policy drafted |
| 2.0 | June 2026 | Kshamtalaya Foundation | Full revision for DPDP Act 2023 and Rules 2025 compliance. Children's data section strengthened. Breach notification updated to 72-hour statutory requirement. Data retention schedule added. DPO section added. Consent requirements expanded. Data Processing Agreement requirement added. All reviewer comments addressed. |