Digital Personal Data Protection Policy

Jaro Institute of Technology Management & Research Limited

Version 1.0 Effective Date: 03rd November 2025

Approved by:

Senior Vice President

Technology & Cross-Functional DPDP Compliance Task Team

Review Frequency: Annually or upon material changes to DPDP Act/Rules

1. Introduction and Purpose

Jaro Education, a publicly listed company on the NSE and BSE, is committed to protecting the personal data of its students, prospects, partners, employees, and other stakeholders. As a Data Fiduciary under the **Digital Personal Data Protection Act, 2023 (DPDP Act)** and the **Digital Personal Data Protection Rules, 2025 (DPDP Rules)** notified by the Ministry of Electronics and Information Technology (MeitY) on November 13–14, 2025, we process significant volumes of digital personal data, including enrollment details, learning progress via our LMS (Jaro Connect/JELXP), CRM records, API integrations with partners (e.g., IIMs, IITs, Wharton, MIT IDSS), and other sensitive educational information.

This **DPDP Policy** outlines our commitment to comply with the DPDP Act and Rules, ensuring lawful, fair, transparent, and secure processing of personal data. It operationalizes a phased implementation aligned with the Rules' rollout:

- **Phase 1** (immediate from November 2025): Governance setup and foundational provisions.
- **Phase 2** (by November 2026): Consent Manager integration.
- **Phase 3** (by May 2027): Full core obligations (consent, rights, security, breach response, etc.).

Compliance safeguards student trust, aligns with SEBI disclosure requirements for listed entities, and mitigates risks of penalties up to ₹250 crore per violation.

2. Scope

This Policy applies to:

- All personal data processed by Jaro Education in digital form (collected online or digitized from offline sources).
- All employees, contractors, vendors, and third-party processors handling personal data on our behalf.
- Processing activities related to our services, including online programs, lead management, learner analytics, and partner collaborations.

It covers Data Principals (students, parents, employees, etc.) in India and extraterritorially where we offer goods/services to Indian residents.

3. Definitions

- **Personal Data**: Any data about an identified or identifiable natural person.
- **Data Principal**: The individual to whom the personal data relates.
- **Data Fiduciary**: Jaro Education (determines purpose and means of processing).
- **Significant Data Fiduciary (SDF)**: Likely applicable due to large-scale student PII processing.
- **Processing**: Collection, storage, use, sharing, erasure, etc.

4. Key Principles

We adhere to DPDP principles:

- Lawful and fair processing.
- Purpose limitation.
- Data minimization.
- Accuracy.
- Storage limitation.
- Integrity and confidentiality (security).
- Accountability.

5. Governance and Accountability

- **Data Protection Officer (DPO)**: Appointed (if SDF classification confirmed) to oversee compliance.
- **DPDP Compliance Task Force**: Cross-functional (Technology, Legal, HR, Data Teams) to monitor implementation.
- **Data Mapping & Inventory**: Comprehensive catalog of personal data flows (e.g., CRM, LMS, Data Lake, Google Drive, APIs) with classification (sensitive for minors).
- **Vendor Management**: Contracts with processors (e.g., AWS, Google, API partners) include DPDP obligations.
- **Training**: Mandatory annual awareness programs for all staff.

6. Notice and Consent

- Provide clear, itemized privacy notices in plain language (English or Eighth Schedule languages) before collection, detailing data categories, purposes, rights, grievance process, and withdrawal mechanisms.
- Obtain free, informed, specific, granular, and withdrawable consent (via portals/apps).
- For children (under 18): Verifiable parental/guardian consent; prohibit harmful behavioural tracking or targeted ads.
- Support Consent Managers (integrate by Phase 2) for centralized consent management.
- Audit and migrate legacy consents; notify users of changes.

7. Data Security and Safeguards

- Implement reasonable security measures: Encryption (at rest/transit), access controls (RBAC, MFA), masking/anonymization, logging, backups, and incident detection.
- Conduct DPIAs for high-risk activities (e.g., AI learner analytics, data lake processing).
- Develop and test breach response plan: Notify Data Protection Board (DPB) and affected Data Principals "without delay" (target within 72 hours).
- Ensure vendor audits and contractual safeguards.

8. Rights of Data Principals

- Enable easy exercise of rights: Access, correction, erasure ("right to be forgotten"), nomination, and grievance redressal.
- Respond to requests within prescribed timelines (e.g., 15 days or as notified).
- Appoint Grievance Officer; provide public contact details and escalation to DPB.
- Implement data minimization and automated erasure when purpose is served.

9. Data Retention and Cross-Border Transfers

- Retain personal data only as long as necessary for purpose (or legal requirements, e.g., 7 years for audits); erase thereafter.
- For cross-border transfers (e.g., to international partners): Permitted unless restricted by government; ensure adequacy and safeguards.
- Maintain logs/traffic data for at least 1 year for breach investigation.

10. Monitoring, Auditing, and Reporting

- Conduct regular internal/external audits.
- Track metrics (consent rates, breaches, rights requests) via dashboards.
- Report to DPB as required (if SDF).
- Document all compliance efforts for accountability and good faith defence.

11. Children's Data

Special protections: Verifiable parental consent, no processing that harms mental well-being, age verification mechanisms.

12. Breach Management

- Immediate containment, assessment, and notification to DPB and affected individuals.
- Maintain incident logs and post-breach reviews.

13. Enforcement and Penalties

Non-compliance may result in penalties up to ₹250 crore. We commit to demonstrating good faith through proactive measures.

14. Review and Updates

This Policy will be reviewed annually or upon changes to DPDP Act/Rules, technology, or business operations. Updates approved by the Task Team and communicated internally.

For queries, contact our Grievance Team at privacy@jaro.in.