Intellectual Property, Data Security and Privacy Policy

Pushpalata Schools

Effective Date: 5/4/2025
Last Updated: 4/4/2025

Pushpalata Schools, including all schools, trusts, societies, educational institutions, branches, and affiliated entities operating under its name or management (hereinafter collectively referred to as the "School", "we", "us", or "our"), recognises that the personal data entrusted to it, particularly data relating to children, is inherently sensitive in nature and requires a high degree of care, confidentiality, and protection.

This Intellectual Property, Data Security and Privacy Policy ("Policy") sets out the principles, practices, and safeguards adopted by the School in relation to the collection, processing, storage, disclosure, retention, and protection of personal data, as well as the protection of intellectual property owned or used by the School. This Policy reflects the School's commitment to lawful, fair, and transparent processing of personal data in accordance with applicable Indian laws and regulations.

Legal Basis and Regulatory Compliance

This Policy has been formulated in accordance with the provisions of the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules"), and is intended to comply with the cyber security directions issued by the Indian Computer Emergency Response Team (CERT-In) dated 28 April 2022. Where Aadhaar data is collected or processed, this Policy is also aligned with the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, and the rules and regulations issued thereunder.

In addition, this Policy is framed having regard to applicable education board requirements (including CBSE, CISCE, and State Boards), child protection norms, and other applicable central and state laws governing educational institutions. This Policy shall be interpreted and applied in a manner consistent with such laws, and nothing contained herein shall be construed as limiting any statutory obligation of the School.

Scope and Applicability

This Policy applies to all personal data processed by the School, whether such data is collected directly from students, parents, guardians, employees, staff members, or other individuals, or received from third parties or government authorities. The Policy applies irrespective of whether the data is processed in physical form or through digital or electronic systems, including but not limited to websites, admission portals, student information systems, enterprise resource planning platforms, learning management systems, cloud-based services, and internal databases.

By accessing the School's website, submitting information through any School-managed platform, or otherwise engaging with the School, individuals acknowledge that they have

read and understood this Policy and consent to the processing of their personal data in accordance with its terms.

Personal Data and Sensitive Personal Data

For the purposes of this Policy, "personal data" refers to any information relating to an identified or identifiable natural person. "Sensitive Personal Data or Information" shall have the meaning assigned to it under the SPDI Rules and includes, inter alia, passwords, financial information, health information, biometric information, and Aadhaar numbers, where applicable.

The School recognises that personal data relating to children requires heightened protection and accordingly applies enhanced safeguards and access restrictions to such data.

Purpose and Nature of Data Collection

The School collects personal data solely for purposes that are lawful, necessary, and directly connected with its educational, administrative, regulatory, and operational functions.

In the case of students and their parents or guardians, personal data is collected primarily during the admission process and thereafter throughout the academic lifecycle of the student. Such data is necessary for processing admissions, maintaining academic records, ensuring student safety and welfare, complying with education board and government requirements, facilitating communication with parents and guardians, and administering scholarships, fee concessions, or government-mandated schemes.

In the case of employees and staff members, personal data is collected for purposes relating to recruitment, employment administration, payroll processing, statutory and regulatory compliance, identity verification, and internal governance.

The School does not collect personal data beyond what is reasonably necessary for the purposes for which it is sought and does not use such data for purposes incompatible with those purposes.

Notice and Consent

At the time of collection of personal data, the School provides clear and meaningful notice regarding the nature of the data being collected, the purpose for which such data is collected, the manner in which it will be used, the entities with whom it may be shared, and the period for which it will be retained.

Consent for the collection and processing of personal data is obtained through admission forms, employment documentation, online portals, or other lawful means. Where consent is withdrawn, the School may continue to retain or process the relevant personal data to the extent required to comply with applicable laws, regulatory requirements, or contractual obligations.

Aadhaar Data Collection and Use

Where Aadhaar information of students, parents, guardians, or staff members is collected, such collection is undertaken strictly in accordance with applicable law and only for purposes that are expressly permitted or mandated, including participation in government-sponsored scholarship, benefit, or welfare schemes such as NPCI (National Payments Corporation of India) Scholarship (Christian / Muslim), Post / Pre Matric Scholarship (Hindu – SC / ST / MBC / DNC), National Scholarship for Std XI & XII (State & Central), ADW Scholarship (Adi Dravidar Welfare) - Post Matric Scholarships (PMS) or similar programmes.

In all such cases, the School ensures that individuals are informed of the purpose of Aadhaar collection, the legal basis for such collection, and the manner in which Aadhaar data will be used. Wherever permissible under law, alternative forms of identification are accepted. Aadhaar numbers, where collected, are stored in a secure and access-restricted manner, are not published or displayed in any public or semi-public form and are retained only for so long as is necessary to fulfil the lawful purpose for which they were collected. The School does not undertake biometric authentication unless expressly authorised under applicable law.

Data Security and Reasonable Security Practices

The School has implemented reasonable security practices and procedures, as required under Rule 8 of the SPDI Rules, to protect personal data from unauthorised access, damage, use, modification, disclosure, or impairment. These practices include a combination of administrative, technical, and physical safeguards appropriate to the nature of the data processed and the size and complexity of the School's operations.

Access to personal data is restricted to authorised personnel on a need-to-know basis, and appropriate authentication and access-control mechanisms are employed. Digital systems are hosted in secure environments, and physical records are stored in controlled locations. The School endeavours, over time, to align its information security practices with recognised standards such as ISO/IEC 27001 or equivalent frameworks, to the extent appropriate.

Cyber Security and CERT-IN Compliance

In accordance with the directions issued by CERT-IN, the School has designated a Point of Contact for cyber security coordination and incident reporting. The School maintains system and network logs in relation to its information and communication technology systems and retains such logs for a minimum period of one hundred and eighty (180) days, or such other period as may be prescribed by law from time to time.

The School has established internal procedures for identifying, reporting, and responding to cyber security incidents, and any reportable incidents are notified to CERT-In within the timelines prescribed under applicable directions. Logs and incident records are stored securely and protected against unauthorised access or tampering.

Data Retention

Personal data is retained only for as long as is necessary to fulfil the purpose for which it was collected, or as required under applicable laws, education board regulations, tax and labour laws, or other statutory or contractual obligations. Upon expiry of the applicable retention

period, personal data is securely deleted, anonymised, or archived in accordance with legal requirements and internal policies.

Disclosure and Sharing of Data

The School may disclose personal data to education boards, government authorities, statutory regulators, courts, or other entities where such disclosure is required or permitted under law. Personal data may also be shared with third-party service providers engaged by the School for operational purposes, provided that such service providers are bound by appropriate confidentiality and data protection obligations.

The School does not sell, rent, or commercially exploit personal data.

Cookies, Log Data, and Website Usage

The School's website may use cookies and similar technologies to enhance functionality, improve user experience, and maintain security. In addition, server logs may automatically record technical information such as IP addresses, browser types, and access times for security, monitoring, and audit purposes. Users may control the use of cookies through their browser settings, subject to potential limitations in website functionality.

Intellectual Property

All intellectual property associated with the School, including but not limited to its name, logo, branding, curriculum materials, academic content, website content, software customisations, and proprietary processes, is the exclusive property of the School or its licensors. No part of such intellectual property may be reproduced, distributed, or used without prior written permission, except as permitted under applicable law.

Rights of Data Principals

Individuals whose personal data is processed by the School have the right to request access to their personal data, seek correction of inaccurate or incomplete information, and raise concerns or grievances regarding the processing of their data. Such requests shall be made in writing and will be addressed in accordance with applicable law.

Grievance Redressal

In compliance with Rule 5(9) of the SPDI Rules, the School has appointed a Grievance Officer to address complaints and concerns relating to personal data and privacy.

Grievance Officer / Data Protection Officer

Name: Mrs. German Jeyarani V
Email: vidyamandir@pushpalata.com

All grievances shall be acknowledged and resolved within thirty (30) days of receipt.

Amendments

The School reserves the right to amend or update this Policy from time to time to reflect changes in law, regulatory guidance, or internal practices. Any such amendments shall take effect from the date of publication of the revised Policy.

Governing Law and Jurisdiction

This Policy shall be governed by and construed in accordance with the laws of India. Courts at Tirunelveli shall have exclusive jurisdiction in relation to any disputes arising out of or in connection with this Policy.