MODERN BABY NURSERY SCHOOL SAMITI

DATA PROTECTION POLICY

2024

JANA BAZAR,AYODHYA

Data Protection Policy for Modern Baby Nursery School Samiti, Jana Bazar, Ayodhya

Purpose:

The purpose of this Data Protection Policy is to establish guidelines for the collection, use, storage, and protection of personal data by Modern Baby Nursery School Samiti. The policy ensures compliance with applicable data protection laws and regulations and safeguards the privacy and rights of all individuals whose data is processed by the organization.

1. Scope:

This policy applies to all employees, volunteers, contractors, and any other individuals who handle personal data on behalf of Modern Baby Nursery School Samiti. It covers all personal data that is collected, stored, processed, or shared by the organization.

2. Policy Statement:

Modern Baby Nursery School Samiti is committed to protecting the privacy and personal data of all students, parents, staff, and other stakeholders. The organization will handle personal data in a lawful, fair, and transparent manner, ensuring that data is collected and processed only for legitimate purposes and is kept secure at all times.

3. Definitions:

Personal Data: Any information relating to an identified or identifiable individual, such as name, address, phone number, email, date of birth, student records, medical information, or any other data that can be used to identify a person.
Data Subject: An individual whose personal data is collected, stored, or processed by the organization.
Data Processing: Any operation performed on personal data, including collection, recording, organization, storage, alteration, retrieval, use, disclosure, transmission, or destruction.
Data Controller: The individual or entity that determines the purposes and means of processing personal data. In this context, Modern Baby Nursery School Samiti is the data controller.

4. Data Collection:

Personal data will only be collected for specific, explicit, and legitimate purposes necessary for the functioning of the school.
Consent will be obtained from data subjects (or their guardians, in the case of minors) before collecting personal data, except where data collection is required by law or necessary to protect vital interests.
Only the minimum amount of personal data necessary for the intended purpose will be collected.

5. Data Use:

Personal data will be used only for the purpose for which it was collected, unless the data subject has given explicit consent for additional use, or such use is required by law.
Examples of data use include managing student enrollment, maintaining academic records, communicating with parents, processing payroll, and ensuring the safety and security of the school community.

6. Data Storage and Security:

Personal data will be stored securely to prevent unauthorized access, loss, or damage. This includes using physical, technical, and administrative safeguards such as secure servers, encrypted storage, access controls, and regular data security training for employees.
Data will be stored only for as long as necessary to fulfill the purposes for which it was collected or as required by law.

7. Data Sharing and Disclosure:

Personal data will not be shared with third parties without the explicit consent of the data subject, except where required by law, regulation, or to protect the vital interests of the data subject.
Data may be shared with authorized third parties, such as service providers or government authorities, only for legitimate purposes and under strict confidentiality agreements.

8. Data Subject Rights:

Data subjects have the following rights regarding their personal data:

Right to Access: Individuals have the right to request access to their personal data held by the organization.
Right to Rectification: Individuals have the right to request correction of inaccurate or incomplete personal data.
Right to Erasure (Right to be Forgotten): Individuals have the right to request the deletion of their personal data in certain circumstances, such as when the data is no longer needed for the original purpose.

Right to Restriction of Processing: Individuals have the right to request the restriction of processing their personal data in certain situations.
Right to Data Portability: Individuals have the right to receive their personal data in a structured, commonly used, and machine readable format and to transmit it to another data controller.
Right to Object: Individuals have the right to object to the processing of their personal data based on legitimate interests or for direct marketing purposes.

9. Data Breach Management:

In the event of a data breach, the organization will take immediate steps to contain and mitigate the breach.
The organization will notify affected individuals and relevant authorities of the breach without undue delay, in accordance with applicable laws.
An internal investigation will be conducted to identify the cause of the breach and implement corrective measures to prevent future incidents.

10. Data Protection Officer (DPO)/IT Personnel:

The organization will appoint a Data Protection Officer (DPO)/IT Personnel responsible for overseeing compliance with this policy, handling data protection queries, and ensuring adherence to data protection laws and regulations.
The DPO /IT will also be responsible for providing training and guidance to staff on data protection practices.

11. Employee Responsibilities:

All employees, volunteers, and contractors are responsible for ensuring that personal data is collected, used, stored, and shared in accordance with this policy and applicable laws.
Employees must immediately report any suspected data breaches or unauthorized access to the Data Protection Officer.
Employees will undergo regular training on data protection and privacy practices.

12. Training and Awareness:

Regular training and awareness sessions will be conducted to ensure that all staff members understand their responsibilities under this policy.
Training will include topics such as data collection, data storage, data security, and recognizing and responding to data breaches.

13. Record Keeping:

The organization will maintain records of data processing activities, including the purposes of processing, types of data collected, retention periods, and any data sharing or transfer activities.
Records will be kept securely and will be accessible only to authorized personnel.

14. Review and Amendment:

This policy will be reviewed annually by the Data Protection Officer and the Governing Body to ensure its effectiveness and compliance with applicable laws and regulations.
Amendments may be made as necessary to address new risks, changes in the law, or evolving best practices in data protection.

15. Grievance Redressal:

Individuals who believe that their personal data has been mishandled or that their rights have been violated may file a complaint with the Data Protection Officer.
The Data Protection Officer will investigate complaints promptly and provide a response within a reasonable timeframe.