Data Protection Policy

1.0 Introduction

Sarvodaya Ashram is committed to protecting the privacy and personal data of its employees, beneficiaries, partners, and all stakeholders. This **Data Protection Policy** establishes the principles, protocols, and legal obligations that govern the collection, processing, and handling of personal data within the organization. This policy is in strict adherence to the latest data protection regulations in India, including the **Digital Personal Data Protection Act, 2023 (DPDP Act)**, which repeals the prior Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

This policy is designed to ensure the lawful, fair, and transparent handling of all personal data, safeguarding it from unauthorized access, misuse, and breach, thereby upholding the trust and privacy rights of every individual.

2.0 Scope and Applicability

This policy applies to all individuals and entities who collect, process, or have access to personal data on behalf of Sarvodaya Ashram, including but not limited to:

- **All permanent, temporary, and contractual employees.**
- **Consultants, volunteers, and interns.**
- **Third-party service providers, vendors, and partners.**

The policy is binding on all work-related activities, whether conducted on Sarvodaya Ashram premises or remotely, and covers all forms of data—digital, physical, and verbal.

3.0 Definitions

- **Personal Data:** As per the DPDP Act, this refers to any data about an individual who is **identifiable** by or in relation to such data.
- **Sensitive Personal Data or Information (SPDI):** A subset of personal data that requires a higher level of protection. This includes, but is not limited to, financial information (bank account numbers, credit/debit card details), biometric data, health conditions, sexual orientation, and medical records.
- **Data Principal:** The individual to whom the personal data relates.
- **Data Fiduciary:** The entity that determines the purpose and means of processing personal data (in this case, Sarvodaya Ashram).

- **Data Processor:** An entity that processes personal data on behalf of the Data Fiduciary.

4.0 Key Principles of Data Processing

Sarvodaya Ashram's data handling practices are guided by the following principles, which are in line with the DPDP Act:

- **Lawfulness, Fairness, and Transparency:** Personal data will only be collected and processed for a lawful purpose. All Data Principals will be informed about the purpose of data collection, their rights, and the identity of the Data Fiduciary.
- **Purpose Limitation:** Data will only be collected for a **specified, explicit, and legitimate purpose**. It will not be used for any purpose incompatible with the original reason for collection.
- **Data Minimization:** Only the **minimum amount of personal data** required to fulfill the stated purpose will be collected and processed. Data that is no longer necessary will be securely deleted.
- **Accuracy:** We will take reasonable steps to ensure that all personal data is **accurate and up-to-date**. Any inaccurate data will be rectified or erased promptly upon request.
- **Storage Limitation:** Personal data will not be retained for longer than is necessary to fulfill the purpose for which it was collected.
- **Integrity and Confidentiality:** We will protect personal data from unauthorized access, loss, or damage through a robust set of security measures.

5.0 Data Collection, Consent, and Security

- **Consent:** The DPDP Act mandates that personal data can only be processed with the **explicit, clear, and informed consent** of the Data Principal. Consent must be a freely given, specific, and unambiguous indication of the Data Principal’s wishes.
- **Legitimate Uses without Consent:** Data can be processed without consent only in specific, defined cases as per the DPDP Act, such as for the performance of a government function, a legal obligation, or a medical emergency.
- **Security Measures:** Sarvodaya Ashram will implement **reasonable security practices and procedures** to protect data. These include:
    - **Access Controls:** Restricting access to personal data to only those individuals who have a legitimate business need.
    - **Encryption:** Using encryption technologies to secure sensitive data both in transit and at rest.
    - **Regular Audits:** Conducting periodic security audits and vulnerability assessments.

- **Data Backup:** Maintaining a regular data backup schedule to ensure the availability and recoverability of information.

6.0 Data Principal's Rights

In accordance with the DPDP Act, every Data Principal has the following rights:

- **Right to Access:** The right to obtain confirmation from the Data Fiduciary on whether their personal data is being processed, and to request a copy of their data.
- **Right to Rectification:** The right to request the correction of inaccurate or incomplete personal data.
- **Right to Erasure:** The right to request the deletion of their personal data, also known as the "right to be forgotten," under certain conditions.
- **Right to Grievance Redressal:** The right to have a readily available mechanism to seek a remedy for any concerns regarding the processing of their personal data.

7.0 Data Breach Response

A **data breach** is a serious incident that can lead to significant harm. Sarvodaya Ashram will follow a structured protocol in the event of any suspected or confirmed data breach:

1. **Immediate Reporting:** Any employee or individual who becomes aware of a data breach must **immediately report** the incident to the designated internal officer.
2. **Investigation:** A thorough and swift investigation will be conducted to assess the cause, scope, and extent of the breach.
3. **Notification:** If the breach is likely to result in a **high risk** to the rights and freedoms of individuals, the affected Data Principals and the **Data Protection Board of India** will be notified without undue delay. The notification will include a description of the breach, its potential consequences, and the measures taken or proposed to be taken to mitigate the risks.

8.0 Training and Review

- **Training:** All employees and stakeholders will undergo **mandatory training** on data protection policies, procedures, and their individual responsibilities.

- **Policy Review:** This policy will be reviewed periodically, at least once a year, to ensure its effectiveness and compliance with evolving data protection laws and best practices.

9.0 Conclusion

Sarvodaya Ashram is resolute in its commitment to protecting personal data and upholding the privacy rights of all individuals. By adhering to this policy, every stakeholder contributes to creating a secure and trustworthy environment, ensuring that data is handled with the utmost care and in full compliance with Indian law.