**Data Protection Policy**

***Policy Number:***

|  |  |
| --- | --- |
| **Prepared and Proposed By**  | Deepa Murali, Advisor, Varshini Illam Trust |
| **Reviewed and Recommended By** | John Alex, Trustee, Varshini Illam Trust |
| **Approved By** | Board Of Trustees |
| **Date of Approval - Ver 1.0** | 06 – 09 - 2025 |
| **Date of last review** | - |
| **Effective Date** | 15 - 09 - 2025 |
| **Review Cycle** | Annually or as recommended by the Board of Trustees |

**List of Contents:**

|  |  |  |
| --- | --- | --- |
| **Sl No** | **Content** | **Page No** |
| 1 | Purpose | 2 |
| 2 | Scope | 2 |
| 3 | Definition | 2 |
| 4 | Data Collection Principles | 2 |
| 5 | Consnet and Guardian Information | 3 |
| 6 | Types of data collected | 3 |
| 7 | Data Storage and Security | 4 |
| 8 | Data Access and Sharing | 4 |
| 9 | Rights of Data Subjects and Guardians | 5 |
| 10 | Roles and Responsibilites | 5 |
| 11 | Breach Notification and Response | 6 |
| 12 | Training  | 6 |
| 13 | Policy Review | 7 |

**1. Purpose**

This Data Protection Policy outlines the principles and procedures by which Varshini Illam Trust (VIT) collects, processes, stores, shares, and protects personal and sensitive data of children with disabilities, their families, and associated stakeholders. This policy ensures compliance with relevant Indian data protection laws and promotes the privacy, dignity, and autonomy of beneficiaries.

**2. Scope**

This policy applies to all employees, volunteers, community workers, therapists, and Trustees of VIT who have access to any personal or sensitive information of children, their families, or associated community members during the course of program delivery and data management.

**3. Definitions**

* **Personal Data**: Any information that relates to an identified or identifiable individual (e.g., name, date of birth, caste, religion).
* **Sensitive Personal Data**: Includes health information, disability status, socio-economic indicators, guardian information, etc.
* **Data Subject**: A child or individual whose personal information is collected.
* **Consent**: Informed, voluntary agreement from a guardian or eligible individual to collect and process data.
* **Processing**: Any operation performed on personal data (collection, storage, use, sharing, disposal).

**4. Data Collection Principles**

All data collection activities undertaken by VIT are governed by fundamental principles designed to protect the privacy, dignity, and rights of the individuals and families served. Data is collected lawfully and fairly, meaning it is gathered only for clearly defined and legitimate purposes, with the informed consent of the child's parent or legal guardian. The Trust ensures transparency in all data-related processes by clearly communicating to beneficiaries what data is being collected, the reasons for its collection, how it will be used, and who will have access to it. In adherence to the principle of data minimization, only data that is directly relevant and necessary for program implementation, service delivery, and assessment is collected, avoiding any unnecessary or excessive information. The Trust is committed to accuracy, ensuring that collected data is regularly reviewed and updated to reflect any changes in the beneficiaries' circumstances. In accordance with the principle of storage limitation, personal data is retained only for as long as it is needed for programmatic, administrative, or legal purposes, after which it is securely deleted or anonymized. To uphold integrity and confidentiality, the Trust implements strict safeguards both technical and organizational to protect data from unauthorized access, alteration, or loss. Personnel with access to sensitive data are trained in confidentiality and ethical data management, and any external entities involved in data processing are required to comply with binding data protection agreements.

**5. Consent & Guardian Information**

Consent for data collection must be obtained from a parent or legal guardian, preferably in writing. In cases where literacy is a barrier, recorded verbal consent is acceptable. The Trust ensures that the age, gender, and relationship of the consent provider to the child are clearly documented. Consent forms are designed to be clear and accessible, outlining the purpose of data collection, the intended use and storage of the data, the rights of the data subject, and the voluntary nature of participation, including the right to withdraw consent at any time without consequences. This process ensures informed, ethical, and respectful engagement with families and caregivers.

**6. Types of Data Collected**

**A. Demographic & Personal Details**

* Child’s full name, DOB, sex, religion, caste
* Family details, sibling data, guardian's information

**B. Geographic & Administrative Data**

* Address, block, panchayat, district
* Program code/category, referral details, admission date

**C. Socio-Economic Status**

* Education, occupation, and income of parents
* Access to government schemes and entitlements

**D. Disability & Education**

* Type of disability, severity, assistive supports
* School enrollment status, access to inclusive education

**E. Health Background**

* Vaccination status, developmental history
* Prenatal, perinatal, and postnatal health events

**F. General Assessment Data**

* Physical measurements, vision, hearing, epilepsy
* Mobility, communication, cognitive understanding
* Activities of daily living, behavioral traits
* Family & community participation
* Preferences and aspirations

**7. Data Storage & Security**

All data collected by VIT is stored and managed with a high level of security to ensure confidentiality, integrity, and protection from unauthorized access or misuse. Digital data is stored on encrypted devices and secure cloud-based platforms that are protected by passwords, firewalls, and access restrictions. Access to digital records is granted only to designated personnel based on their role and responsibilities, ensuring that sensitive information is not exposed unnecessarily.

Physical records, such as consent forms and assessment files, are stored in locked cabinets or secure storage areas within the Trust’s premises. These are accessible only to authorized staff members, and access is tracked and regularly reviewed to prevent unauthorized handling.

Where appropriate, data used for reports, research, or external presentations is either anonymized (removal of personally identifiable information) or pseudonymized (using codes or identifiers in place of names) to protect the identity of children and families.

The Trust also conducts regular data backups to prevent data loss due to hardware failures or system errors. In addition, routine cybersecurity audits and checks are carried out to identify vulnerabilities and strengthen digital security systems. Antivirus software, secure login protocols, and access logs are maintained to monitor data usage and detect any breaches. These measures collectively ensure that personal and sensitive data is handled responsibly and securely at all times.

**8. Data Access and Sharing**

Access to personal and sensitive data collected by VIT is governed by strict internal protocols to ensure that data is only used for its intended purpose and handled by authorized personnel. Internal access to data is restricted to staff members who are directly involved in service delivery, monitoring, assessment, or reporting. These individuals are trained in data confidentiality and are required to follow standard operating procedures that prevent unauthorized access or data misuse.

When external sharing of data is necessary such as with District Early Intervention Centre (DEIC) officials, government departments, policy makers, or project partners such sharing is done in a controlled and responsible manner. Three key conditions must be met:

**Informed Consent:** Prior, written or recorded consent must be obtained from the child’s parent or legal guardian, clearly stating the nature of the data being shared and the purpose of such sharing.

**Anonymization or Pseudonymization:** Wherever possible, data is shared in a de-identified format. This ensures that personal identifiers (such as names, addresses, or identification numbers) are removed, reducing the risk of the child or family being identifiable.

**Data Sharing Agreements:** All external entities receiving data must sign a formal data-sharing agreement, which outlines the scope of access, limitations on use, responsibilities for maintaining confidentiality, and the legal implications of any breach or misuse.

Under no circumstances will VIT sell, trade, or exploit any personal data for commercial purposes. The Trust has a zero-tolerance policy for data misuse, and any breaches of this policy by internal or external parties will lead to strict action, including legal consequences if required.

**9. Rights of Data Subjects and Guardians**

VIT is committed to upholding the rights of data subjects primarily children with disabilities—and their parents or legal guardians, in accordance with ethical standards and applicable data protection laws. The Trust recognizes that individuals whose data is collected have clear entitlements regarding how that data is used, maintained, and safeguarded.

Guardians and data subjects have the right to access the personal and sensitive data that has been collected about them. Upon request, the Trust will provide a copy of the data in a clear and understandable format, along with details on how it has been used or shared.

They also have the right to request correction or deletion of their data if it is found to be inaccurate, outdated, or no longer necessary for program purposes. Such requests will be honored within a reasonable time frame, and appropriate records will be updated or securely deleted from both physical and digital systems.

Guardians have the right to withdraw consent for data collection or use at any time, without fear of retaliation or loss of services. Once consent is withdrawn, the Trust will stop processing the data, except in cases where retention is legally required or justified for safeguarding or operational reasons.

In the unlikely event of a data breach such as unauthorized access, loss, or misuse of personal information the Trust is obligated to promptly inform the affected individuals. The notification will include details of the nature of the breach, data involved, potential risks, and any remedial steps being taken to mitigate harm.

These rights are clearly communicated during the consent process and can be exercised by contacting the designated Data Protection Officer or program representative. Upholding these rights is essential to the Trust’s mission of ensuring dignity, transparency, and trust in all interactions with the communities it serves.

**10. Roles & Responsibilities**

To ensure the effective implementation of data protection practices, VIT assigns specific responsibilities to key personnel involved in data collection, management, and oversight. Each role plays a critical part in safeguarding personal and sensitive information and ensuring the Trust's compliance with ethical and legal standards.

Data Protection Officer (DPO): The DPO is responsible for overseeing the implementation and enforcement of this Data Protection Policy. This includes ensuring compliance with applicable data protection laws and internal guidelines, conducting regular audits, responding to data access or correction requests, and managing incidents related to data breaches. The DPO also serves as the point of contact for beneficiaries and staff regarding any data privacy concerns or grievances.

Therapists & Field Staff: These team members are directly involved in collecting and updating data during therapy sessions, assessments, and home or community visits. They are responsible for ensuring that data is collected ethically, confidentially, and accurately, using approved tools and formats. They must obtain and verify informed consent before collecting any data and are trained to handle sensitive information with discretion.

Community Workers / Anganwadi Teachers: As trusted community-level facilitators, these individuals play a key role in building awareness among families about their rights related to data privacy. They assist in explaining consent forms in local languages or accessible formats, help gather consent from parents or guardians, and support caregivers in understanding how their data will be used. They also act as intermediaries between the Trust and the community to ensure transparency and trust.

Program Coordinators: Program Coordinators are tasked with ensuring that data collection processes follow the Trust’s guidelines and that informed consent is consistently obtained and documented. They oversee the proper training of staff, verify the accuracy and completeness of data, and ensure that only relevant data is collected. They also monitor how data is used for planning, reporting, and service delivery, and coordinate with the DPO for any escalations or policy updates.

**11. Breach Notification and Response**

Any data breach must be reported to the Data Protection Officer within **24 hours**. An investigation will be conducted, and affected families will be informed if necessary. Remedial action will be taken promptly.

**12. Training and Awareness**

To ensure responsible handling of personal and sensitive data, VIT mandates regular training for all staff members, volunteers, and community-level workers involved in data collection, management, or access. These training sessions are integral to building a culture of data protection, accountability, and ethical service delivery.

Training covers core areas including:

**Data Privacy Principles**: Staff and volunteers are educated on the fundamental principles of data privacy such as lawfulness, fairness, transparency, data minimization, accuracy, storage limitation, and confidentiality. These sessions emphasize the importance of respecting the rights of data subjects and safeguarding their information at every stage of the data lifecycle.

**Ethical Data Collection:** Team members are trained on how to collect data ethically and respectfully, especially when working with vulnerable populations such as children with disabilities. This includes guidance on obtaining informed consent, ensuring voluntary participation, communicating data collection purposes in simple language, and maintaining cultural sensitivity during interactions.

**Recognizing and Reporting Data Breaches:** Participants are trained to identify potential data breaches such as unauthorized access, data loss, or misuse and are instructed on the immediate steps to take when such incidents occur. Clear reporting mechanisms are established, with designated staff such as the Data Protection Officer responsible for investigating and responding to any breach.

Training is conducted at the time of onboarding and is refreshed periodically, especially when policies are updated or new data-related procedures are introduced. Attendance is recorded, and participation is mandatory to ensure that all personnel are equipped to handle data with the highest standards of care and compliance.

**13. Policy Review**

This policy will be reviewed annually or upon significant legal or programmatic changes.