

# DATA PROTECTION POLICY

Policy Title	Data Protection Policy
Prepared By	Heena Sharma
Approved By	Inderjot Singh
Approved Date	15 <sup>th</sup> July 2024
Effective Date	15 <sup>th</sup> July 2024
Policy Review Date	01 <sup>st</sup> August 2025

## Data Protection Policy

### 1.Introduction

Small Steps is committed to protecting the privacy and security of the personal data of our students, staff, and parents. This policy outlines the procedures and measures in place to ensure that all data is handled responsibly and in compliance with relevant data protection laws. Our approach to data protection is guided by the principles of confidentiality, integrity, and availability of information.

#### Definitions:

- **Personal Data:** Refers to any information relating to an identified or identifiable individual.
- **Processing:** Encompasses any operation performed on personal data, including its collection, storage, use, and sharing.
- **Children:** Refers to the individuals whose personal data is being recorded.

#### Data Collection:

At Small Steps, we adhere to strict guidelines for the collection of personal data, ensuring it is done only for specified, explicit, and legitimate purposes. The types of personal data we may collect include:

- Contact details (such as name, address, phone number, email)
- Medical and health information
- Educational records
- Behavioural assessments
- Program Specific goals and Objectives
- Emergency contact information

### 2.Purpose of Policy

The purpose of this policy is to provide clear guidelines on the collection, use, storage, and sharing of personal data at Small Steps. This policy applies to all staff, students, and parents and encompasses the use of various applications, including Hirasumus for program data collection, Slack for internal communication, MS Co-pilot & MS One Drive for data and file storage, CURA for safeguarding, Redrock for internal staff training and CEUs, and Photo Circle for sharing videos and photos within our internal network and with parents only.

### 3.Aims and Objectives

At Small Steps, we are committed to maintaining the highest standards of data protection and privacy. Our policy aims to ensure the safe and secure handling of personal data, protecting the privacy and rights of our students, staff, and parents. By providing clear guidelines and establishing robust procedures, we aim to promote a secure environment for data collection, communication, sharing, and storage.

- To ensure the safe and secure handling of personal data in compliance with applicable data protection laws.

- To protect the privacy and rights of our students, staff, and parents.
- To provide clear guidelines on the use of specific applications and tools for data collection and communication.
- To establish procedures for the secure sharing and storage of personal data.

#### 4. Responsibility

This policy applies to all employees, volunteers, contractors, paraprofessionals and third-party service providers who handle personal data on behalf of Small Steps.

#### 5. Policy Components and Implementation

##### 5.1 Data Collection:

At Small Steps, we prioritize the secure and responsible collection of personal data. Our policy ensures that data collection is conducted for specified, explicit, and legitimate purposes, using the following applications and tools:

- **Hirasmus:** Utilized for program data collection. All data entered into Hirasmus must be accurate and relevant. To protect privacy, avoid using full names where possible and use initials or unique identifiers instead.
- **Slack:** Employed for internal communication. Personal information should only be shared in private channels or direct messages on Slack, avoiding public channels.
- **MS Co-pilot and MS OneDrive:** Used for secure file storage and management to safeguard personal data.
- **Redrock Training:** Utilized for internal staff training and Continuing Education Units (CEUs), ensuring staff competence and compliance with data protection protocols.
- **CURA:** Employed as safeguarding software to uphold the safety and well-being of our students, integrating data protection measures.
- **Photo Circle:** Employed for sharing videos and photos within our internal network and with parents. It is crucial to ensure that images and videos do not include students without explicit consent. Blur out or avoid capturing images of students who have not consented to media sharing to protect their privacy.

##### 5.2 Data Sharing and Storage:

- **Secured Network:** Ensure that all data shared online is done through secure, encrypted networks. Avoid using unsecured public Wi-Fi for accessing or sharing personal data.
- **Avoid Public Platforms:** Photos, or videos of students on public platforms or Small Steps social media should be used only after securing a written consent from parents/guardian which should be updated annually. Internal media sharing should be confined to Photo Circle or other approved secure applications and access should only be provided to authorized individuals or clinical staff members.
- **Data Minimization:** Only collect and share the minimum amount of personal data necessary for the intended purpose.

### 5.3 Consent and Privacy:

- **Obtaining Consent:** Ensure that explicit written consent is obtained from parents or guardians before capturing and sharing any photos or videos of students. Keep a record of all consents and update it annually.
- **Anonymization:** Where possible, anonymize data by removing or obfuscating personal identifiers.
- **Access Control:** Limit access to personal data to authorized personnel only. Implement role-based access controls to ensure that individuals only have access to data necessary for their role.

### 5.4 Data Security:

- **Encryption:** Encrypt sensitive data both in transit and at rest to protect it from unauthorized access.
- **Password Protection:** Ensure that all accounts and devices used for data access are protected with strong, unique passwords. Use two-factor authentication where possible.
- **Regular Audits:** Conduct regular audits of data security practices to ensure compliance with this policy and identify areas for improvement.

### 5.5 Incident Response:

- **Reporting Incidents:** Immediately report any data breaches or security incidents to the Case Supervisor or the Center Manager.
- **Incident Handling:** Follow the established incident response plan to contain and mitigate any data breaches. Notify affected individuals and relevant authorities as required by law.

### 6. Review and Monitoring:

This policy will be reviewed annually by the Small Steps Senior Leadership Team and updated as necessary to ensure ongoing compliance with data protection laws and best practices. Small Steps will regularly monitor compliance with this policy through audits, staff training, and feedback from the Small Steps community.

By adhering to this Data Protection Policy, Small Steps aims to promote a culture of data privacy and security, ensuring that the personal information of our students, staff, and parents is always safeguarded.