# Going to School Data Protection Policy for Minors

*Upholding the Privacy, Rights, and Dignity of Children and Young People*

## 1. Introduction

Going to School (GTS) is committed to safeguarding the **privacy, dignity, and data rights of all children and young people** involved in our programs. We recognize that children have a distinct right to protection from exploitation, misuse, or loss of their personal and sensitive information.

This policy establishes the framework for how GTS **collects, stores, uses, secures, and disposes of data** concerning minors (individuals under the age of 18), across all locations and contexts—including schools, internships, media content creation, research, and digital learning platforms.

It applies to all GTS staff, interns, volunteers, vendors, contractors, consultants, trustees, and partner organizations. It also reinforces our organizational commitment to **child safeguarding, digital ethics, and legal compliance**.

## 2. Legal and Regulatory Framework

This policy is grounded in the following laws and rights-based frameworks:

- **The Information Technology Act (2000)** & IT (Reasonable Security Practices) Rules, 2011
- **The Protection of Children from Sexual Offences (POCSO) Act, 2012**
- **Juvenile Justice (Care and Protection of Children) Act, 2015**
- **The Personal Data Protection Bill** (India – pending enactment)
- **Rights of Persons with Disabilities (RPWD) Act, 2016**
- **UN Convention on the Rights of the Child (UNCRC)** – particularly Article 16 (Right to Privacy)
- **National Commission for Protection of Child Rights (NCPCR) Guidelines**

## 3. Scope of the Policy

This policy applies to:

- All children (aged 0–18) who engage in GTS programs (in school, out of school, internships, content creation)

- All data formats: written, visual, digital, biometric, location-based, and behavioral
- All GTS projects: research, media, design, skills education, monitoring & evaluation
- All stakeholders interacting with such data, including GTS employees, creative teams, partner organizations, funders, and evaluators

## 4. Types of Child Data Covered

- **Personally Identifiable Information (PII):** Full name, date of birth, address, school name, ID number
- **Photographs and Media:** Still images, audio recordings, video footage, animation likeness
- **Sensitive Personal Data:** Disability, caste, religion, health records, parental occupation, family income
- **Biometric and Digital Data:** Fingerprints, geotagging, facial recognition, device usage data, chat logs
- **Survey and Research Inputs:** Baseline/endline data, feedback forms, testimonials, storyboards

## 5. Data Protection Principles

GTS follows the **seven foundational principles of ethical data protection**:

1. **Lawful and Transparent Collection**
   Data is collected only after informed consent/assent and used strictly for programmatic needs.
2. **Purpose Limitation**
   Data is used only for the purpose it was collected. No repurposing or secondary use is allowed.
3. **Data Minimization**
   Only the minimum required information is collected—no excess or irrelevant data is stored.
4. **Accuracy and Updating**
   Data is regularly reviewed and corrected to prevent harm due to outdated or incorrect records.
5. **Limited Access and Confidentiality**
   Access to sensitive child data is strictly role-based and documented in audit logs.

6. **Storage Limitation**
   Data is retained only as long as necessary and securely deleted thereafter, as per retention policy.

7. **Child-Centric Consent**
   Consent processes prioritize understanding, dignity, and inclusion of both children and guardians.

## 6. Consent and Assent

- Written **informed consent** from a parent, guardian, or institutional authority is mandatory before collecting or publishing any data about a child.
- Where the child is over **12 years old**, **assent** is also sought—ensuring they understand the purpose, use, and risks involved.
- All consent/assent forms are:
  - Translated into local languages
  - Available in Easy Read and pictorial formats
  - Explained orally by trained staff where literacy or disability is a barrier

Consent is not one-time; it is **renewed** when the purpose or context of use changes.

## 7. Use and Sharing of Data

- Data is used **only** for the purpose it was explicitly collected for (e.g., a TV show, evaluation, curriculum design).
- It is **never shared** with third parties—including donors, sponsors, or collaborators—without:
  - Guardian-signed consent, and
  - A signed data-sharing agreement that includes safeguarding protocols.
- GTS **does not sell, trade, or use child data for profiling, advertising, or political content**.
- All images, videos, or stories used in **external communication (websites, reports, events)** require a separate case-by-case release and must avoid:
  - Revealing location or school name
  - Stigmatizing portrayal of caste, poverty, disability, or gender

## 8. Data Storage and Security

GTS ensures **technical and administrative safeguards** for data protection, including:

- **Encrypted digital storage systems** with two-factor authentication
- **Role-based access** with time-stamped audit logs
- Regular **data backup**, password hygiene training, and device security protocols
- **Paper-based data** (e.g., consent forms) stored in locked cabinets within secure offices
- **Biometric and geotagged data**, if collected, is anonymized and stored separately
- Mandatory **data protection training** for all staff working with children or child data

## 9. Rights of the Child Regarding Their Data

Children and their guardians have the right to:

- **Access**: Review the data collected about them
- **Withdraw Consent**: Request data deletion or discontinue participation at any time
- **Correction**: Request changes to incorrect or misleading information
- **Erasure**: Request removal of their data after the program concludes (unless legally restricted)

These rights are explained in **child-friendly language**, and a trained staff member assists children and guardians in accessing or exercising them.

## 10. Breach Management

If there is a suspected or confirmed data breach:

- The **Data Protection Officer** must be notified within **24 hours**
- Affected children/guardians will be informed immediately
- A **root cause analysis** will be conducted and documented
- Corrective actions (technical or procedural) will be taken within **48–72 hours**
- The breach is reported to appropriate authorities, including **NCPCR**, if harm is suspected

All breaches are recorded in a **Breach Incident Register** and reviewed quarterly.

## 11. Oversight and Review

- The **GTS Data Protection Committee** includes members from safeguarding, legal, digital, and research teams.
- This committee meets **quarterly** to:
  - Review adherence to the policy
  - Analyze risk from evolving technologies (e.g., AI in education)
  - Update protocols based on field realities or legal amendments
- Annual data protection reports are shared with:
  - The **Executive Director**
  - The **Board of Trustees**
  - Independent legal or safeguarding auditors (where applicable)

## 12. Integration with Other Policies

This policy is read in conjunction with:

- **GTS Child Protection & Safeguarding Policy**
- **Whistleblower Policy**
- **POSH Policy**
- **DEI Commitments**
- **Code of Conduct**
- Program-specific data usage protocols (TV, field research, internships)