Going to School Digital Security Policy

Protecting Data | Safeguarding People | Securing Systems

1. Introduction

Digital technology powers how **Going to School (GTS)** delivers its mission—from field data collection to storytelling, donor communications, and internal collaboration. With this opportunity comes risk.

This **Digital Security Policy** outlines how GTS protects its digital systems, data, devices, and users—especially children, communities, and staff—against threats like data breaches, cyberattacks, surveillance, and unethical misuse.

The policy aligns with GTS's **Data Protection Policy for Minors**, **Child Safeguarding Policy**, and **Ethics & Integrity Framework**, and ensures compliance with Indian law and international standards.

2. Purpose

This policy exists to:

- Protect **sensitive and personal data** collected, stored, or shared by GTS
- Prevent **unauthorized access**, loss, or misuse of GTS digital resources
- Guide all users in **safe and ethical digital practices**
- Comply with the **Information Technology Act, 2000**, and relevant Indian data protection rules
- Embed a **culture of digital hygiene, security, and accountability** across the organization

3. Scope and Applicability

This policy applies to:

- All GTS employees, interns, consultants, and volunteers
- All devices and systems owned or used by GTS (phones, tablets, laptops, cloud storage)
- All external vendors, developers, and service providers with access to GTS systems
- All data collected from or shared with children, partners, donors, or the public
- Any digital activity conducted in GTS's name or using its infrastructure

4. Core Principles

- **Confidentiality**: Data and communications are protected from unauthorized access.
- **Integrity**: Data is accurate, complete, and not tampered with.
- **Availability**: Systems are reliably accessible to authorized users.
- **Accountability**: Everyone at GTS is responsible for secure digital behavior.
- **Minimalism**: Only essential data is collected and retained.
- **Consent**: Informed digital consent is obtained where applicable (especially with minors).

5. Roles and Responsibilities

Role	Responsibility
All Staff	Follow safe digital practices, report incidents
IT/Tech Lead	Enforce cybersecurity tools and protocols
Data Protection Officer (DPO)	Oversee digital data security and compliance
HR & Training	Induct staff in digital safety and review annually
External Partners	Comply with GTS digital security clauses and access limits

6. Acceptable Use Guidelines

All staff and collaborators must:

- Use **GTS-authorized devices and platforms** for official communication and data storage
- Use **strong, unique passwords** and change them every 90 days
- Use **multi-factor authentication (MFA)** for email, cloud storage, and CRM systems
- Access data only on **secure, password-protected Wi-Fi**
- Avoid using **personal devices** for storing sensitive data
- Log out of systems when not in use and lock devices in public spaces

- Use GTS-approved cloud tools (e.g., Google Workspace, encrypted folders)
- Use ethical digital behavior when representing GTS online or offline

7. Prohibited Digital Behaviors

- Storing or sharing child data on WhatsApp, personal email, or USBs
- Downloading unapproved software or apps on GTS devices
- Uploading photos/videos of children to social media or third-party servers without consent
- Sharing passwords or device access with unauthorized users
- Using GTS digital systems for illegal or unethical activity
- Taking backups of program data onto personal devices without encryption or approval
- Using AI tools to process data without explicit consent and review

8. Data Protection and Storage

- **All sensitive data** (program, finance, donor, child-related) must be:
  - Encrypted at rest and in transit
  - Stored only in GTS-approved cloud servers with role-based access
  - Retained only as long as necessary, per GTS's data retention schedule
- Child data must be **anonymized** when used in reports or presentations
- Devices used for child interviews or photos must be registered and signed out with supervision
- **Data collected in the field** must be uploaded and deleted from local devices within 48 hours

9. Third-Party Access and Vendor Security

- Vendors and partners must:
  - Sign a **Digital Security & Data Protection Agreement**
  - Be reviewed for compliance with Indian IT rules and GDPR (if applicable)

  - Only access what is needed for contracted work

- GTS may conduct security audits or revoke access at any time if a breach is suspected

10. Incident Reporting and Breach Response

- Any digital security incident (lost device, phishing, unauthorized access) must be reported to the DPO within **2 hours**
- The DPO will:
  - Investigate and assess the impact
  - Notify affected parties if needed
  - Take remedial steps (password resets, revoking access, reporting to authorities)
- Major incidents will be documented, reviewed, and shared with leadership and, where appropriate, donors or legal authorities

11. Training and Awareness

- All staff and volunteers undergo **mandatory digital security training during induction**
- Annual refresher modules cover:
  - Phishing awareness
  - Password hygiene
  - Secure cloud and mobile use
  - Updates on evolving cyber threats
- Field teams receive **specialized guidance on collecting and storing child data safely**

12. Policy Review and Improvement

- This policy is reviewed annually by the **IT and Ethics Team**, with input from the DPO and relevant external advisors
- Feedback from users and incidents will be used to:
  - Update protocols

- Improve software and security layers
- Adapt to new laws, threats, or technologies

13. Alignment with Other GTS Policies

This policy is implemented in tandem with:

- **Data Protection Policy for Minors**
- **Child Protection & Safeguarding Policy**
- **Whistleblower Policy**
- **Code of Conduct**
- **Ethics and Integrity Framework**
- **Volunteer Engagement Policy**

GTS is committed to safeguarding not only children and communities in person, but also their digital identities, stories, and data. Through this policy, we protect the trust placed in us—and build a digital culture that reflects our ethics, responsibility, and vision.