DATA POLICY

SAHAYOG SOCIETY
A-240, INDIRA NAGAR, LUCKNOW

FOREWORD

This Data Policy has been developed by SAHAYOG to reinforce our commitment to responsible data governance, digital integrity, and ethical information practices. As an organization working with diverse stakeholders, we recognize that the information entrusted to us—whether personal, sensitive, or organizational—must be protected and managed with care, transparency, and accountability.

In an era of rapidly evolving technology and legal frameworks, this policy ensures that all employees, consultants, interns, and partners understand their responsibilities when handling data. It outlines the systems in place to protect privacy, secure sensitive content, and respond to incidents with preparedness and integrity.

This policy is not merely a technical document—it is a reflection of our values. Whether it is safeguarding a colleague‟s identity, responsibly using official devices, or ensuring consent before collecting information, these actions uphold the trust that stakeholders place in SAHAYOG.

SAHAYOG needs to save certain information about its employees and their work, and other stakeholders to enable us to maintain adequate records and continuity of work. It is necessary to process and retain such information, so projects may be delivered and legal obligations to funding bodies, government and third-party partners met.

This policy applies to all employees, consultants, and other representatives engaged by SAHAYOG (herein after referred to as ‘employee(s)’). All contractors and agents acting for and on behalf of us should be made aware of this policy. This policy applies to all personal and professional data processed on computers and stored in manual (paper-based) files.

We encourage everyone who engages with SAHAYOG to read this policy carefully and follow it with sincerity. Your cooperation strengthens our collective ability to serve communities more effectively and ethically.

s/d
DIRECTOR
SAHAYOG

CONTENT OF CHAPTERS

Clarification of Terms (2025 Addition)

For this policy, "**data**" includes:

- **Personal data** (such as name, contact details, government ID numbers)
- **Sensitive personal data** (such as health status, caste, religion, or financial information)
- **Organizational data** (such as project reports, photos, research findings)

"**Stakeholders**" include:

- Employees, consultants, volunteers, interns, donors, beneficiaries, and partner organizations

Legal Reference:

- *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 under the IT Act, 2000*
- *Digital Personal Data Protection Act, 2023 (DPDP Act)*

Chapter 1. *General Provisions*

1. Data will be processed lawfully so as not to violate any fundamental rights, fairly and in a transparent manner.
2. For every user, SAHAYOG will provide an official email-id along with a password. It is mandatory to use the official email-id for official SAHAYOG work. The password may be changed by the employee during the term of employment only with permission from and with the knowledge of

SAHAYOG. All the passwords will be known to and saved with the Director of SAHAYOG.

Updated Clause (2025):
Employees should have no expectation of privacy when using SAHAYOG‟s digital infrastructure. However, access to their devices, communications, or records will only occur with due cause and documented authorization from the Director, unless required for urgent operational reasons.

3. The data/files/folders and all official work undertaken during anyone‟s term of employment with SAHAYOG should be stored in well-marked folders on the official laptop/desktop provided. **The employee must return all official data to the organization at the time of departure.** SAHAYOG is authorised to format/delete the data or change laptop/desktop without prior notice, when operationally required. It is the responsibility of the employee to remove any duplicate folders by their name in the organisation‟s external hard disks.
4. No personal data or unofficial downloads are permitted on the official laptop/desktop.
5. Every team should maintain a „materials‟ folder on their official computer/laptop, wherein they save all photos, videos and similar content.
6. For the convenience of employees, SAHAYOG has a catalogue of electronic items like pen drives, external hard disks, a cellphone with a charger, voice recorder, among other items. Employees may issue and use these devices for official purposes by **signing** their name and date of issue on the official register. They will also be required to return the above-mentioned items after completion of the task by **signing** their name and entering the return date. For the duration an employee is in possession of any of the above-mentioned items, they are fully responsible for its safety. In case of mishandling or loss, the employee in possession will be held accountable.
7. Employees are strictly advised against using social or other websites for personal use, while using the office internet, during office hours.
8. Employees may only share any official SAHAYOG related content on their social media pages or handles with prior consent from the organisation.
9. Once an employee hands in their resignation, they are no longer entitled to carry the official laptop, if one has been issued to them, outside the premises of SAHAYOG without prior permission of the administrative team at SAHAYOG.
10. On resigning, an employee is required to hand over all the official data on their laptop/desktop in a secure manner, to the organisation. This data will be transferred to an external hard disk, which will then be verified by the administrative team at SAHAYOG. This process will be carried out in the presence of at least two existing staff members, to be decided by the Director of SAHAYOG.
11. After completion of the notice period, the exiting employee is required to duly remove themselves from any **WhatsApp** or other official SAHAYOG group. In the event of the exiting employee‟s failure to do so, they will be removed from all such group correspondence forums by the organisation.
12. To ensure its processing of data is lawful, fair and transparent, the NGO shall maintain a Register of Systems, which will record where specific data has been saved, when and by whom.

13. Data will be collected and used for many purposes, of which these are the main categories:
    • Obligations under the employment contract (recruitment, training, appraisal, remuneration, welfare etc.)
    • Legitimate business purposes (due diligence, performance monitoring, financial monitoring and decision-making, administration and security arrangements etc.)
    • Legal and regulatory requirements
    • Provision of services to our donor and clients through grant agreements and service contracts with third parties
14. This policy shall be reviewed at least annually.

Chapter 2. *Storage and Handling of Data Records*

All data will be stored on media that ensures their security, integrity, reliability, usability, and authenticity. Storage conditions and handling processes should ensure the records are protected from unauthorised access, loss, or destruction and from theft.

Chapter 3. *Data Access*

Access to records will be governed in a way that reflects needs and requirements and ensure there is no opportunity for the records to be disclosed, deleted, altered or destroyed, either accidentally or intentionally.

Chapter 4. *Consent and Data Subject Rights (2025 Addition)*

SAHAYOG will collect personal or sensitive personal data only after obtaining informed and explicit consent from the individual concerned. The individual will have the right to:

- Access their data
- Request correction
- Withdraw consent (noting that doing so may affect service delivery in some cases)

Legal Reference:
Sections 5 and 6, DPDP Act, 2023

Chapter 5. *Data Breach Notification Protocol (2025 Addition)*

In the event of a suspected or confirmed data breach (e.g., loss, unauthorized access, or theft), SAHAYOG shall:

- Notify the Director and administrative team immediately
- Record the incident in the Register of Systems
- Assess the risk if personal or sensitive personal data is involved
- Notify affected individuals if necessary
- Implement remedial actions to prevent recurrence

Legal Reference:

- *Rule 8(4), SPDI Rules, 2011*
- *Section 8(6), DPDP Act, 2023*

Chapter 6. *Data Retention Timeline (2025 Addition)*

Data shall be retained only as long as necessary to fulfill the purpose for which it was collected or as required by applicable law. After this period, data will be securely deleted or anonymized. Retention periods for various data categories will be defined in SAHAYOG‟s internal Data Retention Schedule.

Legal Reference:
Section 8(7), DPDP Act, 2023

Chapter 7. *Data Protection Awareness (2025 Addition)*

All employees, interns, and consultants will receive training on this Data Policy during onboarding. Periodic refreshers will be provided to reinforce data handling protocols, highlight emerging threats, and clarify responsibilities.

Reviewed and revised by- Gul Srivastava
Date- June, 2025

Approved by- Secretary, Sahayog