Sākshi
EQUALITY IS INCLUSIVENESS

DATA PROTECTION POLICY

OBJECTIVE

The purpose of this policy is to maintain the privacy of and protect the personal information of employees, contractors, vendors, interns, associates, volunteers, beneficiaries, donors, clients and partners of Sakshi and ensure compliance with laws and regulations applicable to Sakshi (hereafter referred to as "the organization").

SCOPE

This Policy applies to all Sakshi employees, interns, associates, consultants, volunteers, beneficiaries, donors, clients, suppliers and partners who receive personal information from Sakshi, who have access to personal information collected or processed by Sakshi, or who provide information to Sakshi, regardless of geographic location.

All employees, consultants, interns and volunteers of Sakshi are expected to support the privacy policy and principles when they collect and / or handle personal information, or are involved in the process of maintaining or disposing of personal information.

This policy provides the information to successfully meet the organization's commitment towards data privacy. All partner firms and any Third-Party working with or for Sakshi, and who have or may have access to personal information, will be expected to have read, understand and comply with this policy. No Third Party may access personal information held by the organization without having first entered into a confidentiality agreement.

This data protection policy ensures that Sakshi

- Complies with data protection law and follow good practice
- Protects the rights of staff, donors, beneficiaries and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

GENERAL STAFF GUIDELINES

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Sakshi will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.

- Personal data should not be disclosed to unauthorised people, either within the organisation or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

DATA STORAGE

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

Storage of hardcopy data

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

Storage of Electronic data

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a DVD, USB or HARD DRIVE), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing service.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smartphones.
- Data belonging to a partner organization or client is stored on a limited access drive separately from other organizational data.
- All servers and computers containing data should be protected by approved security software and a firewall.

Sākshi
EQUALITY IS INCLUSIVENESS

ACCESSING PERSONAL DATA

All individuals who are the subject of personal data held by Sakshi are entitled to:

- Ask what information Sakshi holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how Sakshi is meeting its data protection obligations.

PERSONAL DATA OF DONORS

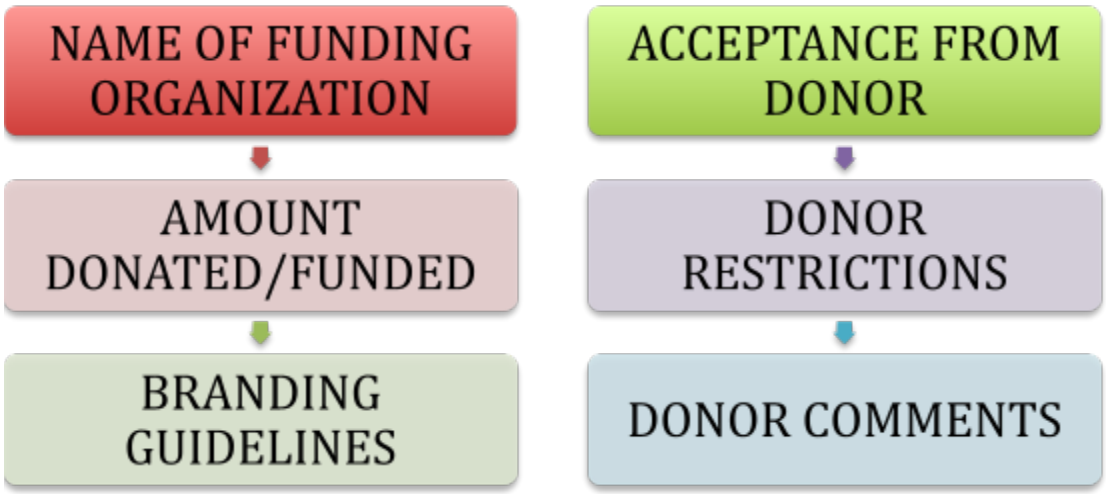
We follow the 9 Donor rights system to ensure that there is a transparency of the data management process. Sakshi's donors have the full right to

1. Be informed of Sakshi's mission, of the way Sakshi intends to use donated resources, and of its capacity to use donations efficiently for their envisioned resolutions
2. Be informed of the identity of those serving on Sakshi's governing board, and to believe the board to apply judicious judgment while carrying out their accountabilities
3. Have an access to Sakshi's current financial statements
4. Obtain appropriate acknowledgment and recognition
5. Be assured that information about their donations is held with respect and with utmost discretion to the degree offered by law
6. Expect that all relationships with individuals representing Sakshi to the donor will be professional
7. Choose to be up-to-date whether those seeking donations are volunteers, employees of the organization or hired solicitors
8. Request to get their names deleted from mailing lists that Sakshi may intend to share
9. enquire while making a donation and to receive prompt, honest and candid answers

INFORMATION COLLECTED BY SAKSHI

For the purposes of processing payments and communicating with donors about Sakshi as well as conducting fundraising and other operations of Sakshi, we utilize information gathered from our donors.

This information includes the following:



FINANCIAL INFORMATION

1. Donations via cheque - Data visible on the cheque should be kept confidential.

2. Donation via Payment Processors and Other Service Providers – In such cases, Payment processors allow donors to offer electronically using a payment services account, a credit card, or other payment methods. These processors collect certain information from donors, and we consult their privacy policies to determine their practices.

3. We also arrange for delivering our donors the finest feasible experience via the service providers we work with (such as: organizations that help non-profit organizations with fundraising). We may share Donor Data and other information with, or have it transmitted by them.

DATA RETENTION

Employee Documents: All employee related documentation is to be retained while the employee continues and 6 Years after termination of employment. Employee payment invoices are to be retained for 8 Years.

Financial Documents: All Financial Documents like Contracts, Bills and Invoices etc. are to be retained for a period of 8 Years.

DATA DISPOSAL

All data should be disposed of when it is no longer necessary for our use, provided that the disposal does not conflict with our data retention policies, our associates' data retention policies, a court order, or any of our regulatory obligations.

- All employees, vendors, and contractors are instructed to not use the following media to store confidential information.
    - paper-based media
    - USB Drives or External Backup programs
    - CD ROM drives.
- All cloud-based storage media being decommissioned should be sanitized when it is no longer necessary, provided that there is a backup of data on production systems to comply with our associates' data retention and contractual obligations.
- Laptop-based storage media may not be donated or sold. All laptop-based storage media should be sanitized prior to the transfer of ownership to a co-worker or prior to destruction.

Date Issued / Revised : 1st April 2020

End of Document