THE SAGE FOUNDATION

Data Privacy Policy

FOR INTERNAL USE ONLY — Not for external distribution

Policy Title	Data Privacy Policy
Document ID	SF-PRIV-INT-2025-01
Version	2.0
Effective Date	January 1, 2026
Next Review	January 1, 2027
Owner	HOD- Technology
Classification	CONFIDENTIAL
Applies To	All staff, volunteers, trustees, interns & contractors of Sage Foundation

⚠ Confidentiality Notice

- This document is strictly for internal use by authorized Sage Foundation personnel.
- Do not share, reproduce, or distribute any portion outside the organization without Board approval.
- Violations may result in disciplinary action and/or legal consequences.

1. Purpose

The Sage Foundation is committed to protecting the personal data of all individuals who interact with our organization — including students and beneficiaries, donors, volunteers, staff, trustees, and program partners. This Internal Data Privacy Policy establishes the rules, responsibilities, and practices that govern how the Foundation collects, processes, stores, and protects personal data across all internal operations.

This Policy exists to:

- Ensure every member of the Sage Foundation team understands their individual responsibilities regarding personal data
- Establish a consistent internal framework for data governance and accountability
- Protect the Foundation from legal, reputational, and operational risks associated with data misuse
- Build and maintain trust with students, donors, partners, and the broader community
- Align internal practices with applicable data protection legislation

© 2026 The Sage Foundation. Confidential & Internal. Do not distribute externally.

2. Scope & Applicability

This Policy applies to ALL individuals operating within or on behalf of the Sage Foundation, including:

Who It Applies To	Examples
Full-time & Part-time Staff	Program coordinators, admin staff, finance team
Board of Trustees	All trustees and honorary members
Volunteers	Event volunteers, program facilitators, mentors
Interns & Fellows	Academic interns, research fellows
Third-party Contractors	IT vendors, auditors, legal counsel, consultants
CSR Program Associates	Individuals working within the CSR Module on behalf of the Foundation

This Policy covers all personal data processed in digital and physical formats, across all devices, systems, and locations where Foundation work is conducted, including remote and off-site settings.

3. Key Definitions

For the purposes of this Policy, the following terms apply:

Term	Definition
Personal Data	Any information relating to an identified or identifiable natural person (e.g. name, ID number, email, location, IP address)
Sensitive Personal Data	Special categories: health records, financial details, religious beliefs, biometric data, data of minors
Data Subject	Any individual whose personal data is being processed (students, donors, staff, volunteers, etc.)
Data Controller	The Sage Foundation determines the purpose and means of processing personal data
Data Processor	A third party that processes data on the Foundation's behalf (e.g. cloud providers, payroll systems)
Processing	Any operation on personal data collection, recording, storage, use, sharing, deletion, and more
Data Breach	Unauthorized access, disclosure, alteration, destruction, or loss of personal data

© 2026 The Sage Foundation. Confidential & Internal. Do not distribute externally.

Term	Definition
DPO	Data Protection Officer, responsible for overseeing compliance with this Policy
Consent	Freely given, specific, informed, and unambiguous agreement to data processing

4. Data Governance & Roles

4.1 The Foundation as Data Controller

The Sage Foundation acts as the Data Controller for all personal data collected through its programs, operations, and CSR activities. As Data Controller, the Foundation determines why and how personal data is processed, and is ultimately responsible for ensuring compliance with this Policy and applicable law.

4.2 Data Protection Officer (DPO)

The Foundation shall designate a Data Protection Officer (DPO) responsible for:

- Monitoring compliance with this Policy and data protection laws
- Advising staff and leadership on data protection matters
- Serving as the point of contact for data subject rights requests
- Managing data breach response and regulatory notifications
- Conducting and overseeing staff data privacy training
- Maintaining the Foundation's data register and processing records

Contact: The DPO can be reached via the Executive Director's office or at the designated privacy contact listed in Section 13.

4.3 Staff Responsibilities

Every individual covered by this Policy shares responsibility for data protection. Specific obligations include:

- Handling personal data only in accordance with this Policy and any role-specific guidelines
- Never accessing personal data beyond what is required for your designated duties
- Reporting suspected data breaches or policy violations immediately to the DPO
- Participating in mandatory data privacy training
- Not sharing, forwarding, or downloading personal data to unauthorized personal devices or external accounts
- Following the Foundation's clean-desk and screen-lock practices when handling physical or digital data

4.4 Trustees & Senior Leadership

The Board of Trustees provides governance oversight of data protection. Senior leadership is responsible for allocating adequate resources for data protection activities, approving this Policy annually, and ensuring a culture of privacy accountability throughout the organization.

© 2026 The Sage Foundation. Confidential & Internal. Do not distribute externally.

5. Personal Data Held by the Foundation

The Foundation processes personal data across several operational categories:

Data Category	Examples	Who It Relates To
Identity & Contact	Name, address, email, phone number	All data subjects
Student & Beneficiary	Academic records, enrollment status, program outcomes, parental consent	Students & families
Donor & Financial	Donation amounts, payment info, tax IDs, bank details	Donors & supporters
Volunteer & Staff	Employment records, payroll, emergency contacts, background checks	Staff & volunteers
Health & Sensitive	Disability info, dietary requirements, safeguarding records	Staff, volunteers, students
CSR Program Data	Partner contacts, program metrics, engagement records	Partner orgs & CSR contacts
Digital & Technical	IP logs, system access records, email communications, device IDs	All users of Foundation systems
Photographic / Media	Event photos, program videos, testimonials	Individuals photographed/recorded

Sensitive personal data (health, financial, safeguarding records) must be treated with additional care and requires explicit consent or a clear legal basis before processing. Only the DPO and authorized role-holders may access sensitive categories.

6. Core Data Protection Principles

All personal data processed by the Foundation must comply with the following principles. These are non-negotiable and apply to every team member:

1 **Lawfulness, Fairness & Transparency**
We only process data with a valid legal basis and inform data subjects clearly about how their data is used.

2 **Purpose Limitation**
Data collected for one purpose must not be used for a different, incompatible purpose without fresh consent or legal basis.

© 2026 The Sage Foundation. Confidential & Internal. Do not distribute externally.

3	**Data Minimisation** We collect only the minimum data necessary for the stated purpose. If you don't need it, don't collect it.
4	**Accuracy** We maintain accurate, up-to-date records. Inaccurate data must be corrected or deleted without delay.
5	**Storage Limitation** Personal data is retained only as long as necessary. Expired data must be securely deleted per the retention schedule.
6	**Integrity & Confidentiality** Data must be protected against unauthorized access, accidental loss, or damage through appropriate security measures.
7	**Accountability** The Foundation, and every individual within it, is responsible for demonstrating compliance with these principles.

7. Lawful Basis for Processing

Every instance of data processing must be supported by at least one of the following legal bases. Staff must consult the DPO if uncertain which applies:

- Consent — The data subject has given clear, voluntary, and specific consent
- Contract — Processing is necessary to fulfil a contract or take pre-contractual steps
- Legal Obligation — Processing is required by applicable law or regulation
- Vital Interests — Processing is necessary to protect someone's life
- Legitimate Interests — The Foundation has a genuine interest that outweighs data subject rights (assessed case-by-case)
- Public Task — Processing in the public interest, particularly for educational programs

For sensitive personal data, processing requires additional grounds such as explicit consent, employment law obligations, or substantial public interest. The DPO must be consulted before processing any sensitive data.

8. Information Security Requirements

8.1 Technical Controls

- All Foundation systems must use strong password authentication (minimum 12 characters, MFA where available)

© 2026 The Sage Foundation. Confidential & Internal. Do not distribute externally.

- Personal data transmitted electronically must be encrypted using TLS/SSL or equivalent
- Data stored on portable devices (laptops, USB drives) must be encrypted at rest
- Access to personal data systems is granted on a least-privilege, need-to-know basis
- All access is logged; logs are reviewed quarterly by the DPO or IT custodian

8.2 Physical Controls

- Physical documents containing personal data must be stored in locked cabinets
- Clean-desk policy applies to all workstations — no personal data left unattended
- Visitors must not have unsupervised access to areas where personal data is stored or processed
- Printed documents containing personal data must be shredded when no longer needed

8.3 Organizational Controls

- Only authorized personnel with a legitimate business need may access personal data
- All staff must complete mandatory data privacy training on joining and annually thereafter
- Third-party processors must sign a Data Processing Agreement before accessing Foundation data
- Personal data must never be shared via personal email accounts or unencrypted messaging apps

9. Data Retention Schedule

Personal data must not be retained longer than necessary. The following schedule applies across all Foundation departments:

Data Type	Retention Period	Disposal Method
Student / Beneficiary Records	Program duration + 5 years	Secure deletion / physical shredding
Donor & Financial Records	7 years (regulatory)	Secure deletion / certified destruction
Staff Employment Records	Duration of employment + 7 years	Secure deletion / shredding
Volunteer Records	Last activity date + 3 years	Secure deletion
CSR Partner Records	Partnership end + 7 years	Secure deletion / shredding
Event Photos & Media (consented)	5 years or until consent withdrawn	Permanent deletion from all systems
Board & Meeting Minutes	Permanent (archive)	Archival storage — restricted access
Incident / Breach Records	5 years from date of incident	Secure deletion
Digital Access Logs	12 months rolling	Automated purge / secure deletion

© 2026 The Sage Foundation. Confidential & Internal. Do not distribute externally.

Data Type	Retention Period	Disposal Method
Marketing & Comms Consent	Until consent withdrawn + 1 year	Secure deletion

10. Data Breach Response Procedure

A data breach is any unauthorized or accidental access, disclosure, alteration, loss, or destruction of personal data. ALL suspected breaches — however minor — must be reported immediately.

If you suspect a data breach, act immediately:

- STOP any further processing or access to the affected data
- REPORT to the DPO and your line manager within 1 hour of discovery
- DO NOT attempt to fix, delete, or cover up the breach before reporting
- PRESERVE all evidence — do not modify files, emails, or system records

10.1 Breach Response Steps

1. Immediate containment — isolate affected systems or data as directed by the DPO
2. Internal assessment — DPO assesses scope, nature, and risk level of the breach within 24 hours
3. Regulatory notification — If required by law, report to the relevant Data Protection Authority within 72 hours
4. Individual notification — Notify affected data subjects where the breach is likely to cause significant harm
5. Root cause analysis — Investigate how the breach occurred and document findings
6. Corrective action — Implement measures to prevent recurrence
7. Post-incident review — DPO and leadership review the response and update procedures as needed

All breach records must be documented and retained for 5 years per the retention schedule.

11. Handling Data Subject Rights Requests

Any individual whose data the Foundation processes may exercise their rights under applicable law. All such requests received by any staff member must be forwarded to the DPO within 24 hours of receipt.

Right	What It Means	Our Deadline
Access	Provide a copy of all personal data we hold about the requester	30 calendar days

© 2026 The Sage Foundation. Confidential & Internal. Do not distribute externally.

Right	What It Means	Our Deadline
Rectification	Correct inaccurate or incomplete data	30 calendar days
Erasure ('Right to be Forgotten')	Delete data where no legal basis exists to retain it	30 calendar days
Restriction	Pause processing while a dispute is resolved	Immediate hold; resolve within 30 days
Portability	Provide data in a structured, machine-readable format	30 calendar days
Objection	Stop processing based on legitimate interest or direct marketing	Immediate for marketing; 30 days for others
Withdraw Consent	Remove consent for consent-based processing	Immediate cessation

12. Special Protections — Children & Sensitive Data

12.1 Children (Under 18)

As an education-focused organization, the Foundation regularly interacts with minors. The following additional safeguards are mandatory:

- Written parental or guardian consent is required before collecting any data from or about a child
- Children's data may only be used for the specific educational or program purpose for which consent was given
- No photographs or media of children may be shared publicly without explicit parental consent
- Data related to children must be stored in restricted-access, encrypted systems
- Any safeguarding concern involving a child's data must be escalated immediately to the DPO and relevant authority

12.2 Sensitive / Special Category Data

The following data types carry additional legal obligations and require explicit consent or a specific legal basis:

- Health and medical information
- Financial hardship or assistance records
- Religious, ethnic, or cultural background (only where relevant to program eligibility)
- Biometric data (e.g. fingerprints, facial recognition — not to be used without Board approval)
- Criminal records or background check results (limited to safeguarding contexts)

Access to special category data is restricted to designated role-holders and must be approved in advance by the DPO. Any unauthorized access to sensitive data is a serious disciplinary matter.

13. Training & Awareness

© 2026 The Sage Foundation. Confidential & Internal. Do not distribute externally.

Data privacy awareness is a shared organizational responsibility. The Foundation requires:

- Induction Training: All new staff, volunteers, and contractors must complete data privacy training before handling any personal data
- Annual Refresher: All covered individuals complete annual data privacy refresher training
- Role-specific Training: Staff handling sensitive data (finance, HR, student records) receive additional specialized training
- Breach Simulation: The DPO conducts an annual data breach simulation exercise to test readiness

Training completion records are maintained by the DPO and reviewed by the Board annually. Failure to complete mandatory training may result in restricted system access.

14. Third-Party & Vendor Management

Where the Foundation engages external parties to process personal data on its behalf (cloud storage, payroll, CRM, grant management systems), the following controls apply:

- A Data Processing Agreement (DPA) must be signed before any data is shared
- The DPO must vet and approve all new data processors before engagement
- Processors are permitted to use data only for the purposes specified by the Foundation
- Processors must have equivalent security measures in place
- The Foundation reserves the right to audit processor compliance at any time
- Upon termination of the relationship, processors must return or destroy all Foundation personal data

The DPO maintains a register of all approved third-party processors, reviewed semi-annually.

15. Internal Contacts & Escalation

Data Protection Officer	Niccon Ghosh
DPO Email	it@shahanigroup.com
IT / Systems Custodian	it@shahanigroup.com
HR / People Team	hr@shahnigroup.com
Finance Team	accounts@shahanigroup.com
Foundation Website	https://thesagefoundation.org/

For urgent breach incidents outside office hours, contact the DPO or Executive Director directly via the emergency contact register held by the office administrator.

© 2026 The Sage Foundation. Confidential & Internal. Do not distribute externally.

16. Policy Review & Amendments

This Policy is owned by the Board of Trustees and managed day-to-day by the DPO. It is reviewed:

- Annually, at the start of each fiscal year
- Following any significant data breach or near-miss
- When there are material changes to applicable law or Foundation operations
- When new categories of personal data are introduced

Amendments are approved by the Board and communicated to all staff in writing, with a minimum of 14 days' notice before taking effect. All previous versions are archived by the DPO for audit purposes.

Internal Acknowledgement & Sign-Off

I confirm that I have read, understood, and agree to comply with the Sage Foundation Internal Data Privacy Policy.

Full Name: NICCON GHOSH **Role / Department:** HOD TECHNOLOGY & IT INFRA

Date: 02-01-2026

Signed acknowledgement copies are retained by HR and reviewed annually by the DPO.

© 2026 The Sage Foundation. Confidential & Internal. Do not distribute externally.