

Samaritan's Fellowship Foundation Pakistan (SFFP)

PRIVACY & DATA PROTECTION POLICY

(Last amended July 2023)

1. PURPOSE

Samaritan's Fellowship Foundation Pakistan (SFFP) recognizes privacy and responsible management of personal information as fundamental components of human dignity, human rights, digital rights and responsible organizational practice. SFFP collects and processes information in connection with its programs, humanitarian assistance, human-rights activities, community engagement, research, advocacy, fundraising, communications, employment, partnerships and digital activities.

This policy establishes SFFP's principles and minimum requirements for collecting, using, storing, sharing, protecting and disposing of personal information. SFFP is committed to ensuring that personal information is processed responsibly, securely, transparently and only for legitimate organizational purposes.

Particular care will be taken where information relates to:

- Children;
- Women and vulnerable persons;
- Survivors of violence or abuse;
- Human-rights defenders;
- Community activists;
- Participants in civic-space activities;
- Persons facing discrimination or persecution;
- Beneficiaries of sensitive programs;
- Staff and volunteers;
- Donors and partners.

2. POLICY STATEMENT

SFFP will seek to ensure that personal information is:

1. Collected for legitimate and clearly defined purposes;
2. Limited to what is reasonably necessary;
3. Accurate and kept appropriately up to date;
4. Used transparently and responsibly;
5. Protected against unauthorized access, disclosure, alteration, loss or destruction;
6. Retained only for as long as reasonably necessary;
7. Shared only where there is a legitimate and authorized basis;
8. Handled with additional safeguards where information is sensitive or high-risk;
9. Processed in a manner consistent with human-rights and digital-rights principles.

SFFP will not knowingly sell personal information or use personal information for unauthorized commercial purposes.

3. SCOPE

This policy applies to personal information processed by SFFP in any form, including:

- Paper records;
- Electronic files;
- Databases;
- Email;
- Websites;
- Online forms;
- Mobile applications;
- Cloud platforms;
- Messaging platforms;
- Donor-management systems;
- CRM systems;
- Research databases;
- Photographs and videos;
- Audio recordings;
- Case files;
- Surveys and assessments;
- Monitoring and evaluation systems.

It applies to:

- Board members;
- Employees;
- Consultants;
- Volunteers;
- Interns;
- Researchers;
- Field personnel;
- Contractors;
- Partners;
- Service providers;
- Any person authorized to access SFFP information.

4. DEFINITIONS

4.1. Personal Information

Information relating to an identified or identifiable individual.

This may include:

- Name;
- Address;

- Telephone number;
- Email address;
- Identification information;
- Photographs;
- Video or audio recordings;
- Employment information;
- Online identifiers;
- Device or technical information;
- Location information;
- Information provided through forms or surveys.

4.2. Sensitive Personal Information

Information that could create significant risk, harm, discrimination, retaliation or loss of privacy if misused or disclosed.

Depending on the context, this may include:

- Health information;
- Biometric information;
- Information concerning children;
- Information about abuse or exploitation;
- Case information;
- Human-rights information;
- Information concerning political or civic activities;
- Information relating to persecution or threats;
- Financial information;
- Identity documents;
- Passwords or authentication information;
- Other information requiring heightened protection.

4.3. Processing

Any operation performed on personal information, including collection, recording, organization, storage, use, analysis, disclosure, transfer or deletion.

4.4. Data Breach

A security incident involving the unauthorized access, disclosure, alteration, loss, destruction or compromise of personal information.

5. PRIVACY AND HUMAN RIGHTS

SFFP recognizes privacy as an important element of human dignity and civic freedom. In human-rights and civic-space programs, inappropriate disclosure of personal information may expose individuals to:

- Harassment;
- Intimidation;

- Discrimination;
- Retaliation;
- Surveillance;
- Social stigma;
- Financial harm;
- Physical or psychological harm.

SFFP will therefore consider the potential human-rights consequences of data processing, particularly where information concerns vulnerable communities, human-rights defenders, survivors or civic actors.

6. DATA PROTECTION PRINCIPLES

SFFP applies the following principles.

6.1. Lawfulness and Fairness

Personal information should be processed through a legitimate and transparent organizational process and not in a manner that is unjust, deceptive or harmful.

6.2. Purpose Limitation

Information should be collected for specified and legitimate purposes and should not be reused for unrelated purposes without appropriate justification or authorization.

6.3. Data Minimization

SFFP will seek to collect only information that is reasonably necessary for the relevant purpose.

6.4. Accuracy

SFFP will take reasonable steps to ensure that important personal information is accurate and appropriately updated.

6.5. Storage Limitation

Personal information should not be retained indefinitely without a legitimate reason.

6.6. Security

Reasonable technical, organizational and administrative safeguards should be used to protect information.

6.7. Confidentiality

Access to personal information should be limited to individuals who have a legitimate need to access it.

6.8. Accountability

SFFP will seek to maintain appropriate records, procedures and responsibilities to demonstrate responsible data management.

7. COLLECTION OF PERSONAL INFORMATION

SFFP will seek to explain, where reasonably practicable:

- What information is being collected;
- Why it is being collected;
- How it will be used;
- Who may receive it;
- How it will be protected;
- How long it may be retained;
- Where appropriate, how individuals may raise questions or requests concerning their information.

Information should not be collected merely because it is technically possible to collect it.

8. CONSENT

Where consent is used as the basis for collecting or using personal information, SFFP will seek to ensure that consent is:

- Informed;
- Voluntary;
- Specific to the relevant purpose;
- Understandable;
- Appropriately documented where necessary.

Consent should not be obtained through coercion, deception or unreasonable pressure. Where appropriate, individuals should be able to withdraw consent, subject to legitimate legal, contractual or organizational requirements.

Consent is not always the only legitimate basis for processing information. SFFP may process information where necessary for legitimate organizational purposes, contractual obligations, safeguarding, legal obligations, protection of individuals, donor requirements or other lawful purposes, subject to applicable law and organizational procedures.

9. CHILDREN'S DATA

Children's personal information requires heightened protection.

SFFP will seek to:

- Collect only information reasonably necessary;
- Obtain appropriate authorization or consent where required;
- Use age-appropriate explanations;
- Limit access;

- Protect children's identities;
- Avoid unnecessary publication of identifying information;
- Apply additional security measures;
- Consider the best interests of the child.

Photographs, videos, names, locations and personal stories involving children must be assessed carefully before publication.

10. SENSITIVE HUMAN-RIGHTS INFORMATION

SFFP may encounter information relating to human-rights violations, persecution, abuse, exploitation, discrimination, threats or other sensitive matters. Such information should be treated as confidential and accessed only by authorized personnel. Where disclosure could create risk, SFFP may use:

- Anonymization;
- Pseudonymization;
- Removal of identifying details;
- Aggregated information;
- Restricted-access systems;
- Secure communication channels.

The safety of individuals must take priority over publicity or storytelling objectives.

11. HUMAN-RIGHTS DEFENDERS AND CIVIC ACTORS

Where SFFP works with human-rights defenders, civic actors, journalists, researchers, activists or community representatives, the organization will consider heightened digital and physical-security risks.

SFFP will seek to avoid unnecessarily recording or publishing:

- Personal addresses;
- Private telephone numbers;
- Identity-document information;
- Precise locations;
- Sensitive affiliations;
- Private communications;
- Information concerning family members;
- Information that could facilitate harassment, surveillance or retaliation.

12. PHOTOGRAPHS, VIDEOS AND STORIES

Photographs, videos, testimonials and personal stories are personal information when individuals can be identified. Before public use, SFFP should consider:

- Whether appropriate consent has been obtained;
- Whether publication creates foreseeable risk;
- Whether the person's identity needs to be disclosed;

- Whether location information should be removed;
- Whether children or vulnerable persons require additional protection;
- Whether the content could cause stigma, retaliation or discrimination.

Consent alone does not eliminate the need for a safeguarding and privacy risk assessment.

13. DATA SECURITY

SFFP will implement reasonable safeguards appropriate to the sensitivity and volume of information being processed.

Security measures may include:

- Password protection;
- Multi-factor authentication where available;
- Role-based access;
- Access restrictions;
- Secure cloud platforms;
- Device security;
- Encryption where appropriate;
- Secure backups;
- Malware protection;
- Software updates;
- Secure disposal;
- Staff awareness and training.

Access should be granted according to the principle of least privilege, meaning individuals should receive only the level of access necessary for their responsibilities.

14. ACCESS CONTROL

SFFP will seek to ensure that:

- User accounts are individually assigned where practicable;
- Passwords are not unnecessarily shared;
- Access is removed when personnel leave or change roles;
- Sensitive files have restricted permissions;
- Administrative access is limited;
- Access to sensitive information is reviewed periodically.

Personnel must immediately report suspected unauthorized access.

15. CLOUD SERVICES AND THIRD-PARTY PLATFORMS

SFFP may use third-party technology platforms for:

- Email;
- Cloud storage;
- Collaboration;

- Fundraising;
- Donor management;
- Communications;
- Website management;
- Data analysis;
- Design;
- Research;
- Program delivery.

Before using third-party platforms for sensitive information, SFFP should consider, as appropriate:

- Security controls;
- Privacy practices;
- Data-storage arrangements;
- Access controls;
- Contractual terms;
- Data-sharing practices;
- Data retention;
- Relevant geographic or cross-border considerations;
- Risks to affected individuals.

SFFP will seek to avoid transferring sensitive information to platforms where appropriate safeguards cannot reasonably be established.

16. AI AND ARTIFICIAL INTELLIGENCE

SFFP recognizes that AI systems can create significant opportunities as well as privacy and data-protection risks. SFFP personnel must exercise particular caution when using AI tools to process personal information.

Personnel must not enter sensitive personal information into public or third-party AI systems unless:

- There is an authorized organizational purpose;
- Appropriate privacy and security risks have been assessed;
- The relevant system is considered suitable for the information;
- Appropriate safeguards are in place;
- Required authorization has been obtained.

Sensitive information that should receive heightened protection includes:

- Beneficiary case details;
- Human-rights case information;
- Children's information;
- Health information;

- Identity documents;
- Information concerning threats or persecution;
- Confidential staff information;
- Passwords and credentials;
- Private communications.

AI outputs involving personal information must also be reviewed for:

- Accuracy;
- Bias;
- Unintended disclosure;
- Inference of sensitive information;
- Hallucinated or fabricated information;
- Unfair or discriminatory conclusions.

AI must not be treated as an automatic authority for sensitive decisions affecting individuals. Where AI contributes to a decision with significant consequences for a person, appropriate human review must remain in place.

17. DATA SHARING

Personal information should only be shared where there is an appropriate and legitimate reason. Before sharing information, SFFP personnel should consider:

- Why the information is being shared;
- Whether the recipient needs the information;
- Whether less information could achieve the same purpose;
- Whether consent or another appropriate basis is required;
- Whether sharing could create a safety or human-rights risk;
- Whether the recipient has adequate safeguards.

Sensitive information should not be shared through insecure or unauthorized channels.

18. PARTNERS AND SERVICE PROVIDERS

Where external partners, consultants or service providers process personal information on behalf of SFFP, appropriate contractual or operational safeguards should be considered.

Depending on the relationship, agreements may address:

- Permitted use of information;
- Confidentiality;
- Security requirements;
- Access controls;
- Restrictions on onward sharing;
- Data retention;
- Incident reporting;
- Secure deletion or return of information.

SFFP will seek to work with service providers that demonstrate appropriate information-security and privacy practices.

19. CROSS-BORDER AND INTERNATIONAL DATA TRANSFERS

SFFP may interact with international donors, partners, platforms and service providers. Where personal information may be transferred or accessed across borders, SFFP will consider:

- The sensitivity of the information;
- The destination and recipient;
- Security arrangements;
- Contractual protections;
- Applicable legal requirements;
- Potential risks to affected individuals.

Particular caution should be exercised where information concerns human-rights cases, vulnerable persons, civic actors or other sensitive matters.

20. DATA RETENTION

SFFP will retain personal information only for as long as reasonably necessary for:

- Program implementation;
- Safeguarding;
- Financial accountability;
- Legal or regulatory requirements;
- Donor reporting;
- Organizational records;
- Research or historical purposes where appropriate.

Where information is no longer required, SFFP should securely delete, destroy, anonymize or otherwise appropriately dispose of it. Retention periods may vary according to the nature and sensitivity of the information.

21. DATA SUBJECT RIGHTS AND REQUESTS

Subject to applicable law and legitimate organizational limitations, individuals may have rights concerning their personal information, including the ability to:

- Ask what personal information is held about them;
- Request correction of inaccurate information;
- Ask questions about how their information is being used;
- Request deletion where appropriate;
- Withdraw consent where consent is the relevant basis;
- Raise concerns regarding inappropriate processing.

Requests should be directed to **SFFP Data Protection Contact:** info@sffp.org.pk

SFFP will respond to reasonable requests within an appropriate timeframe, taking into account applicable legal requirements, security considerations and the rights of other individuals.

22. DATA BREACH AND SECURITY INCIDENT RESPONSE

A suspected or confirmed data breach must be reported promptly to the appropriate SFFP authority.

Examples include:

- Lost or stolen device containing personal information;
- Unauthorized access to an account;
- Accidental disclosure of personal information;
- Hacked email or cloud account;
- Malware or ransomware incident;
- Unauthorized download of sensitive files;
- Misdirected email containing confidential information;
- Loss of paper records;
- Unauthorized publication of personal information.

SFFP will seek to:

1. Contain the incident;
2. Protect affected individuals;
3. Assess the nature and severity of the breach;
4. Identify information affected;
5. Restrict further unauthorized access;
6. Document the incident;
7. Take corrective measures;
8. Notify relevant persons or authorities where required or appropriate.

23. PRIVACY INCIDENTS INVOLVING HUMAN-RIGHTS CASES

Where a breach concerns human-rights cases, survivors, witnesses, activists or vulnerable communities, SFFP will conduct a heightened risk assessment.

The response should consider whether disclosure could result in:

- Retaliation;
- Physical danger;
- Legal or social consequences;
- Harassment;
- Discrimination;
- Loss of livelihood;
- Psychological harm;
- Further exposure of a survivor or victim.

Protecting the affected person's safety and dignity will be a central consideration in the response.

24. RESEARCH AND DATA COLLECTION

Research and monitoring activities involving personal information should be designed according to data-minimization and risk principles.

Researchers and field personnel should:

- Explain the purpose of data collection;
- Collect only relevant information;
- Protect participant identities;
- Use secure storage;
- Avoid unnecessary sensitive information;
- Obtain appropriate consent or authorization;
- Apply appropriate anonymization;
- Assess potential consequences of disclosure.

Where research concerns vulnerable communities or sensitive human-rights issues, additional safeguards should be applied.

25. COMMUNICATIONS, FUNDRAISING AND PUBLIC DISCLOSURE

SFFP may use stories, photographs, testimonials and program information for legitimate communication and fundraising purposes.

However, communications must not unnecessarily expose individuals to:

- Shame;
- Stigma;
- Retaliation;
- Discrimination;
- Physical or digital risk.

SFFP will seek to ensure that fundraising objectives do not override privacy, dignity or safeguarding considerations.

26. SOCIAL MEDIA AND DIGITAL COMMUNICATION

Personnel representing SFFP must exercise care when sharing information through:

- Social media;
- Email;
- Messaging applications;
- Online meetings;
- Websites;
- Digital campaigns.

Personal information should not be published through organizational channels without appropriate authorization.

Private conversations, confidential documents and sensitive case information must not be forwarded or posted without authorization.

27.EMPLOYEE AND VOLUNTEER INFORMATION

SFFP may collect personal information relating to staff, volunteers, consultants and applicants.

Such information may include:

- Contact information;
- Employment history;
- Qualifications;
- Identification information;
- Payroll or financial information;
- Performance information;
- Emergency contacts.

Access to personnel information will be limited according to legitimate organizational needs.

28.DONOR AND PARTNER INFORMATION

Donor and partner information will be used for legitimate organizational purposes, including:

- Donation processing;
- Communication;
- Reporting;
- Compliance;
- Relationship management;
- Financial records.

SFFP will seek to protect donor and partner information against unauthorized disclosure.

29.DATA ACCURACY AND CORRECTION

SFFP will take reasonable steps to maintain accurate information where accuracy is important to program delivery, safeguarding, financial administration or legal compliance.

Personnel should correct material errors when identified.

30.TRAINING AND AWARENESS

SFFP will provide appropriate privacy and data-protection awareness to personnel whose responsibilities involve personal information.

Training may include:

- Privacy principles;
- Secure handling of personal information;
- Password and account security;

- Phishing and social-engineering awareness;
- Digital safety;
- Data minimization;
- Safe communications;
- Human-rights case confidentiality;
- Children's data;
- Photography and media;
- Cloud platforms;
- Responsible AI use;
- Data-breach reporting.

31. RESPONSIBILITIES

- **Board / Governing Body:** Provides oversight and supports organizational accountability for privacy and data protection.
- **Leadership:** Ensures that reasonable systems, responsibilities and resources are in place.
- **Data Protection Focal Point:** Coordinates privacy matters, supports implementation, maintains relevant records and assists with incidents and requests.
- **Managers:** Ensure personnel understand applicable data-protection responsibilities.
- **Personnel:** Every individual handling SFFP information is responsible for protecting it and reporting suspected breaches.
- **Third Parties:** Partners, contractors and service providers must follow applicable contractual and organizational requirements when processing SFFP information.

32. DATA PROTECTION BY DESIGN

SFFP will seek to consider privacy and data protection at the planning stage of new programs, systems, surveys, databases, digital tools and technology projects.

Where appropriate, planning should consider:

- What information is genuinely required;
- Whether the information can be anonymized;
- Who needs access;
- How information will be protected;
- How long it will be retained;
- What could happen if the information is disclosed;
- Whether technology introduces additional privacy or human-rights risks.

33. HIGH-RISK DATA PROCESSING

Additional safeguards should be considered when processing information that could create significant risks to individuals.

Examples include information concerning:

- Human-rights violations;
- Persecution;
- Threats;
- Survivors;
- Children;
- Health;
- Legal matters;
- Civic or advocacy activities;
- Vulnerable communities;
- Identity documents;
- Financial hardship;
- Sensitive locations.

Where appropriate, SFFP may conduct a privacy or data-protection risk assessment before collecting or processing such information.

34.ACCOUNTABILITY AND DOCUMENTATION

SFFP will seek to maintain appropriate documentation concerning:

- Significant data-processing activities;
- Consent where required;
- Data-sharing arrangements;
- Data breaches;
- Privacy requests;
- Risk assessments;
- Relevant third-party providers;
- Data-retention arrangements.

Documentation should be proportionate to organizational size, resources and risk.

35.NON-COMPLIANCE

Failure to comply with this policy may create risks to individuals and to SFFP.

Depending on the circumstances, violations may result in:

- Additional training;
- Corrective action;
- Restriction of system access;
- Disciplinary action;
- Termination of employment or engagement;
- Contractual action;
- Notification to relevant authorities where appropriate or required.

Serious or deliberate misuse of personal information may constitute misconduct.

36. POLICY REVIEW

This policy will be reviewed periodically and may be updated in response to:

- Changes in applicable law or regulatory requirements;
- Emerging digital-rights standards;
- New technology;
- Artificial intelligence developments;
- New organizational programs;
- Data-security incidents;
- Donor or partner requirements;
- Organizational learning.

The policy should be reviewed at least every two years, or earlier where circumstances require.

37. COMMITMENT

Samaritan's Fellowship Pakistan recognizes that **privacy is not merely a technical or administrative issue; it is an important element of dignity, freedom, security and human rights.**

SFFP is committed to responsible data stewardship and to protecting individuals from avoidable harm arising from the collection, use, storage or disclosure of personal information. As SFFP expands its work in digital rights, AI, technology, civic participation and human-rights advocacy, the organization will continue strengthening its privacy and data-protection practices.

People's rights, dignity and safety remain central to how SFFP collects, uses and protects information.