FAITH ACTION AND WORK SILC (FAWS)

DATA PROTECTION POLICY

Background

Faith Action and Work SILC (FAWS) Women Organization is a non-profit-making organization for and led by women, bringing together People Living with HIV (PLHIV) in all their diversities through support groups. FAWS was formed in 2007 and registered by the Department of Social Services under the Ministry of Gender and Children with registration No. NCC/SD/CBO/087. Over the years, FAWS has built its capacity, mentored communities, and led advocacy using a practical, experience-based approach, earning significant experience and a growing reputation as a local organization representing PLHIV in health advocacy and human rights issues. Guided by its vision of "Healthy Communities," FAWS seeks to empower Women Living with HIV and vulnerable communities through inclusive and sustainable development initiatives, strategic partnerships, advocacy, and capacity strengthening that improve quality of life

Vision

Healthy communities

Mission

To empower women living with HIV and vulnerable communities through inclusive sustainable development initiatives,strategic partnerships, advocacy, and capacity strengthening and improve quality of life.

Core values

Quality –we are committed to advocate for quality services for PLHIVs at all levels

Team work -we value and build strong teams that generate synergy and commitment

Integrity -we uphold openness transparency and mutual accountability

Policy Owner	Coordinator/Director
Governance Oversight	Board of Management
Effective Date	_____
Approved Date	_____
Review Date	_____
Version	1.0
Status	For Board Approval

Confidentiality Notice: This policy is an internal FAWS governance document.

1. INTRODUCTION

Faith Action and Work SILC (FAWS) recognizes that personal data is an important organizational asset and that individuals have rights and legitimate expectations regarding the privacy, security and responsible use of information about them. FAWS is committed to handling personal data lawfully, fairly, transparently, securely and responsibly in all its programmes, operations and partnerships.

This Policy establishes the governance framework and minimum requirements for the collection, use, storage, access, disclosure, transfer, retention and secure disposal of personal data processed by or on behalf of FAWS. It is intended to protect data subjects, reduce organizational risk, and support accountability to employees, volunteers, beneficiaries, donors, partners, suppliers and other stakeholders.

2. PURPOSE

The purposes of this Policy are to:

- Ensure that FAWS processes personal data in accordance with applicable Kenyan data protection and privacy requirements and relevant contractual obligations.
- Protect the confidentiality, integrity and availability of personal data.
- Provide clear responsibilities and minimum controls for staff, volunteers, Board members, consultants, interns, contractors and partners.
- Ensure that personal data is collected only for specified, legitimate purposes and is adequate, relevant and limited to what is necessary.
- Protect data subjects from unauthorized access, misuse, loss, theft, alteration, disclosure or destruction of their personal data.
- Establish processes for responding to data subject requests, complaints and personal data breaches.
- Promote a culture of privacy, confidentiality, accountability and responsible information management.
- Support FAWS in meeting donor, statutory, contractual, programme and reporting requirements without compromising data protection obligations.

3. SCOPE

This Policy applies to:

- All FAWS employees, Board members, management, volunteers, interns, consultants, contractors and temporary personnel.
- All personal data processed by FAWS, whether in paper, electronic, photographic, audio, video or other form.
- All FAWS offices, field activities, programmes, projects, outreach activities and partner-supported activities.
- All devices, systems, databases, cloud services, email accounts, mobile phones, tablets, computers, removable media and communication platforms used to process FAWS personal data.
- All third parties that process personal data on behalf of FAWS, to the extent provided for in contracts or other binding arrangements.

4. LEGAL AND REGULATORY FRAMEWORK

This Policy shall be implemented with reference to applicable laws, regulations, guidance and contractual requirements, including:

- The Constitution of Kenya, including the right to privacy.
- The Data Protection Act, 2019 (No. 24 of 2019).
- Applicable Data Protection Regulations issued under the Data Protection Act, including the Data Protection (General) Regulations, 2021 and the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021, where applicable.
- Applicable employment, financial, statutory reporting and records-management requirements.
- Donor agreements, partner agreements, confidentiality agreements and other contractual obligations applicable to FAWS.
- Applicable guidance and directions issued by the Office of the Data Protection Commissioner (ODPC).

Where a conflict arises between this Policy and a mandatory legal or regulatory requirement, the applicable law or regulatory requirement shall prevail. Management shall seek appropriate professional advice where the application of a legal requirement is uncertain.

5. KEY DEFINITIONS

Term	Meaning
Personal Data	Information relating to an identified or identifiable natural person.
Sensitive Personal Data	Personal data requiring enhanced protection, including health, financial, biometric and other categories recognized as sensitive under applicable law.
Data Subject	An identified or identifiable individual whose personal data is processed.
Processing	Any operation performed on personal data, including collection, recording, organization, storage, retrieval, use, disclosure, transfer, restriction or destruction.
Data Controller	A person or organization that determines the purpose and means of processing personal data.
Data Processor	A person or organization that processes personal data on behalf of a data controller.
Consent	A freely given, specific, informed and unambiguous indication of an individual's wishes by which the individual agrees to processing of personal data concerning them, where consent is the applicable lawful basis.
Personal Data Breach	A security incident involving accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to personal data.
Data Protection Lead	The person designated by FAWS management to coordinate implementation of this Policy and related data protection activities. This role does not automatically imply that the person is a statutory Data Protection Officer unless formally designated as such.
Third Party	An individual or organization outside FAWS that receives, accesses or processes FAWS personal data.

6. DATA PROTECTION PRINCIPLES

FAWS shall apply the following principles when processing personal data:

- Lawfulness, fairness and transparency – personal data shall be processed on an appropriate lawful basis and in a manner that is fair and understandable.
- Purpose limitation – data shall be collected for specified, explicit and legitimate purposes and not used incompatibly with those purposes.
- Data minimization – only data that is adequate, relevant and necessary for the stated purpose shall be collected or used.
- Accuracy – reasonable steps shall be taken to keep personal data accurate and up to date.
- Storage limitation – personal data shall not be kept longer than necessary, subject to legal, donor, contractual and operational requirements.
- Integrity and confidentiality – appropriate safeguards shall protect personal data against unauthorized or unlawful processing and against accidental loss, destruction or damage.
- Accountability – FAWS shall be able to demonstrate compliance through policies, procedures, records, training, controls and reviews.

7. DATA GOVERNANCE AND RESPONSIBILITIES

Effective data protection is a shared responsibility. The following governance arrangements shall apply:

- Board of Management: Approves this Policy, provides oversight, promotes accountability, reviews significant data protection risks and receives material compliance or breach reports.
- Coordinator/Director: Ensures implementation, allocates appropriate resources, enforces compliance and escalates significant risks to the Board.
- Data Protection Lead: Coordinates the implementation of this Policy; maintains the data protection action plan and relevant registers; advises management; coordinates data subject requests, breach response, training and periodic compliance reviews; and serves as the primary internal contact for data protection matters.
- ICT/Systems Responsible Person: Implements appropriate technical safeguards, access controls, backups, malware protection, patching, system security and incident support.
- Finance and Administration: Protects personnel, payroll, procurement, supplier and financial information and ensures appropriate records management.
- Programme/M&E Teams: Collect and use programme and beneficiary data only for authorized purposes, apply data minimization, protect source documents and ensure responsible data sharing.
- Employees, Volunteers, Interns and Consultants: Follow this Policy and related procedures, maintain confidentiality, use data only for authorized work and promptly report incidents.
- Partners and Service Providers: Process FAWS personal data only for authorized purposes and under appropriate contractual and security requirements.

8. DATA INVENTORY AND RECORDS OF PROCESSING

FAWS shall maintain, proportionate to its size and activities, an inventory or register of significant personal data processing activities. The register should identify, where applicable:

- Categories of data subjects.
- Categories of personal and sensitive personal data.
- Purposes and lawful basis for processing.
- Sources of the data.

- Persons or categories of recipients with whom data may be shared.
- Systems, locations and storage arrangements.
- Retention periods or retention criteria.
- Key risks and safeguards.
- Third-party processors and relevant agreements.

9. DATA COLLECTION AND LAWFUL PROCESSING

FAWS shall:

- Collect personal data only for specified and legitimate organizational, programme, statutory, contractual or administrative purposes.
- Provide appropriate information to data subjects about the collection and intended use of their data, through a privacy notice or other suitable communication where required.
- Determine and document an appropriate lawful basis for processing before processing begins, including consent where consent is required and appropriate.
- Avoid collecting information merely because it may be useful in the future.
- Use approved forms, registers, systems and data collection tools.
- Verify information where reasonably necessary and correct inaccurate information.
- Apply enhanced safeguards when collecting or processing sensitive personal data.
- Ensure that field teams collect only information necessary for the activity and securely transmit records to approved systems.

10. CONSENT

Where consent is the lawful basis for processing, FAWS shall ensure that consent:

- Is freely given and not obtained through coercion or inappropriate pressure.
- Is informed, specific and understandable.
- Is recorded in an appropriate form where evidence of consent is required.
- Can be withdrawn through a reasonably accessible process, subject to lawful grounds for continued processing where applicable.
- Is not assumed merely because an individual participates in a programme or receives a service.
- Is not used as a substitute for another more appropriate lawful basis where consent is not the correct basis.

For photographs, videos, testimonials, publications, fundraising materials or other communications where consent is required, FAWS shall use an appropriate consent process and shall respect any limitations communicated by the data subject.

11. PRIVACY NOTICES AND TRANSPARENCY

FAWS shall provide clear and appropriate information to data subjects regarding:

- Who is collecting or processing the information.
- The purpose for which the information is collected.
- The categories of information collected.

- The applicable lawful basis where appropriate.
- Who may receive or access the information.
- How long the information will be retained or the criteria used to determine retention.
- The rights available to the data subject and how to exercise them.
- The appropriate FAWS contact for privacy questions, requests or complaints.

12. DATA SECURITY

FAWS shall implement technical, physical and organizational safeguards appropriate to the nature and risk of the personal data processed.

Physical safeguards may include:

- Locked cabinets and restricted records rooms.
- Controlled access to offices and records storage areas.
- Visitor controls where appropriate.
- Secure transport and custody of physical records.
- Secure disposal of paper records.

Electronic safeguards may include:

- Strong passwords and, where feasible and appropriate, multi-factor authentication.
- Role-based access controls and least-privilege access.
- Approved antivirus/anti-malware and firewall protections.
- Regular security updates and patching.
- Regular backups and appropriate recovery arrangements.
- Encryption or other appropriate protection for sensitive information in transit or at rest where feasible.
- Secure configuration of computers, phones, tablets and cloud systems.
- Logging and monitoring proportionate to the systems and risks.

Organizational safeguards may include:

- Confidentiality obligations and agreements.
- Staff induction and periodic data protection awareness.
- Segregation of duties.
- Access reviews and user-account management.
- Incident response procedures.
- Periodic risk assessments and compliance reviews.

13. ACCESS CONTROL AND CONFIDENTIALITY

- Access to personal data shall be granted on a need-to-know and role-based basis.
- User access shall be removed or adjusted promptly when staff leave, transfer roles or no longer require access.
- Staff shall not share passwords or use another person's account.
- Personal data shall not be accessed out of curiosity or for unauthorized personal purposes.
- Confidential information shall not be discussed in public places where it may be overheard.

- Confidentiality obligations continue after employment, volunteering, consultancy or Board service ends.

14. USE OF EMAIL, WHATSAPP, MOBILE DEVICES AND CLOUD SERVICES

Because FAWS may conduct field and programme activities using mobile communication and electronic platforms:

- Personal data shall be shared electronically only through approved and reasonably secure channels.
- Sensitive beneficiary information should not be posted in open groups or shared with persons who do not have an authorized need to know.
- Where WhatsApp or similar platforms are used for operational coordination, staff shall minimize personal data, avoid unnecessary identifiers and delete or move information to approved systems where appropriate.
- Personal devices used for FAWS work should have a screen lock, current security updates and other reasonable safeguards.
- Loss or theft of a device containing FAWS personal data shall be reported immediately.
- FAWS shall avoid storing official records solely on an individual employee's personal device or personal cloud account.
- Bulk emails containing personal information shall be handled carefully to prevent unintended disclosure.

15. DATA SHARING AND DISCLOSURE

FAWS may share personal data where there is a lawful and authorized basis, including where:

- Required or permitted by law.
- Necessary to meet a legitimate programme, contractual, statutory or donor requirement and consistent with applicable data protection obligations.
- The data subject has provided valid consent where consent is the appropriate basis.
- A competent authority lawfully requests the information.
- A service provider is processing the information on FAWS's behalf under appropriate safeguards.

Before sharing personal data, FAWS shall consider necessity, proportionality, confidentiality, security, the recipient's authority and the risks to data subjects. Unnecessary or excessive data shall not be shared.

16. THIRD-PARTY DATA PROCESSORS AND PARTNERS

Where a third party processes personal data for FAWS or receives personal data from FAWS, FAWS shall, where appropriate:

- Conduct proportionate due diligence on the third party's data protection and security arrangements.
- Enter into an appropriate written agreement containing data protection and confidentiality requirements.
- Specify the purpose and permitted scope of processing.
- Require appropriate technical and organizational safeguards.
- Require prompt notification of suspected or actual personal data breaches.
- Require cooperation with data subject requests, investigations and compliance obligations where applicable.

- Require secure return or deletion of data at the end of the engagement, subject to lawful retention requirements.

17. CROSS-BORDER DATA TRANSFERS

Where FAWS transfers or permits access to personal data outside Kenya, the transfer shall be assessed and implemented in accordance with applicable Kenyan data protection requirements, including any applicable requirements relating to safeguards, adequacy, consent, contractual arrangements or other lawful mechanisms. The Data Protection Lead shall maintain a record of material cross-border transfers.

18. DATA SUBJECT RIGHTS AND REQUESTS

Subject to applicable law and lawful limitations, data subjects may have rights including:

- To be informed about the use of their personal data.
- To access personal data held about them.
- To request correction or rectification of inaccurate or incomplete information.
- To object to certain processing.
- To request deletion or erasure where applicable.
- To request restriction of processing where applicable.
- To withdraw consent where consent is the lawful basis.
- To exercise other rights available under applicable law.

FAWS shall:

- Provide a reasonable mechanism for submitting requests.
- Verify identity where necessary to protect against unauthorized disclosure.
- Log and track requests.
- Respond within applicable legal timelines.
- Escalate complex or disputed requests to management and, where necessary, obtain legal or specialist advice.
- Avoid deleting or altering records merely to defeat a lawful request or investigation.

19. DATA RETENTION AND RECORDS MANAGEMENT

FAWS shall retain personal data only for as long as reasonably necessary to meet the purpose for which it was collected or applicable legal, statutory, donor, contractual, audit, safeguarding or accountability requirements.

Each relevant department shall maintain or contribute to a retention schedule specifying:

- Record category.
- Purpose of retention.
- Responsible department or custodian.
- Retention period or retention criteria.
- Secure disposal method.
- Any legal, donor or contractual hold that prevents disposal.

Where a record is subject to litigation, investigation, audit, donor review or another legitimate hold, disposal shall be suspended until the hold is lifted.

20. SECURE DISPOSAL

When personal data is no longer required and no retention obligation applies, FAWS shall securely dispose of it through methods appropriate to the medium and sensitivity, including:

- Cross-cut shredding or secure destruction of paper records.
- Secure deletion of electronic files and accounts.
- Secure wiping or destruction of storage media where necessary.
- Deletion of redundant copies held on approved systems where appropriate.

21. PERSONAL DATA BREACH MANAGEMENT

Any actual, suspected or potential personal data breach shall be reported immediately to the Data Protection Lead, Coordinator/Director or designated management contact. Examples include loss or theft of a device, accidental disclosure, sending information to the wrong recipient, unauthorized access, hacking, malware, unauthorized alteration or destruction of personal data.

FAWS shall maintain a documented breach response process that includes:

1. Immediate reporting and recording of the incident.
2. Initial assessment of what happened, what information was affected and who may be affected.
3. Immediate containment and recovery measures.
4. Assessment of risks and potential harm to data subjects.
5. Escalation to the Coordinator/Director and Board Chairperson where the incident is material.
6. Notification to the ODPC and affected data subjects where required by applicable law.
7. Documentation of decisions, actions, communications and corrective measures.
8. Post-incident review and implementation of measures to prevent recurrence.

FAWS shall maintain awareness of the statutory requirement to notify the ODPC of a notifiable personal data breach without delay and within the applicable legal timeframe. Current ODPC materials identify a 72-hour notification period for relevant breaches after the controller becomes aware of the breach. Where FAWS acts as a processor, contractual and legal notification obligations shall also be observed.

22. DATA PROTECTION IMPACT ASSESSMENTS AND PRIVACY BY DESIGN

FAWS shall consider privacy and data protection risks before introducing new systems, projects, technologies or processing activities that may create significant risks to individuals.

- A Data Protection Impact Assessment (DPIA) shall be considered where required by law or where the processing is likely to create significant risks to data subjects.
- New systems and programme tools should collect the minimum necessary information.
- Privacy and security safeguards should be incorporated at the design stage rather than added only after implementation.
- High-risk processing should be escalated to management and, where appropriate, specialist or legal advice obtained.

23. TRAINING AND AWARENESS

FAWS shall provide data protection and confidentiality awareness appropriate to personnel roles. Training should cover:

- Data protection principles and staff responsibilities.
- Confidentiality and appropriate access.
- Secure use of email, phones, WhatsApp and cloud systems.
- Handling of beneficiary and sensitive information.
- Data breach identification and reporting.
- Data subject rights and requests.
- Secure disposal and records management.

Training and awareness activities shall be documented.

24. MONITORING, AUDIT AND COMPLIANCE

FAWS shall periodically assess compliance with this Policy through proportionate measures such as:

- Review of access rights.
- Checks on physical and electronic records.
- Review of data-sharing arrangements.
- Review of retention and disposal practices.
- Incident and breach trend analysis.
- Staff awareness checks.
- Periodic internal audits or management reviews.

Material non-compliance shall be reported to the Coordinator/Director and, where appropriate, the Board of Management. Corrective actions shall be assigned to responsible persons and tracked to completion.

25. COMPLAINTS AND ESCALATION

Any individual who believes their personal data has been mishandled by FAWS may raise a concern through the designated FAWS contact. Complaints shall be handled fairly, confidentially and without retaliation.

- The complaint shall be recorded and acknowledged where appropriate.
- Relevant facts and records shall be reviewed.
- The complainant shall receive an appropriate response within applicable timelines.
- Unresolved or serious matters shall be escalated to management.
- Where required or appropriate, the complainant may be informed of available external remedies, including the ODPC complaint process.

26. NON-COMPLIANCE AND DISCIPLINARY ACTION

Failure to comply with this Policy may expose FAWS and individuals to operational, contractual, reputational and legal risks. Depending on the nature and seriousness of the breach, FAWS may take corrective or disciplinary action in accordance with applicable employment contracts, HR policies, agreements and law.

- Counselling, retraining or corrective instruction.
- Restriction or withdrawal of system access.
- Disciplinary action under applicable procedures.
- Termination of contracts or engagements where justified.
- Referral to relevant authorities where required by law.

27. POLICY REVIEW AND APPROVAL

This Policy shall be reviewed at least every three (3) years, or earlier where there are material changes in law, regulation, technology, organizational structure, programme activities, donor requirements or significant data protection incidents.

The Coordinator/Director shall coordinate the review and submit proposed amendments to the Board of Management for approval. The Board may require an earlier review whenever it considers this necessary.

28. DOCUMENT CONTROL

Version	Date	Description	Prepared/Reviewed By	Approved By
1.0	_____	Initial Board-ready policy	_____	Board of Management

29. APPROVAL

This Policy was considered and approved by the FAWS Board of Management.

Policy Name	FAWS Data Protection Policy
Approved By	Board of Management
Board Meeting/Minute Reference	_____
Approval Date	_____
Effective Date	_____

Chairperson – Name	_____
Chairperson – Signature	_____
Coordinator/Director – Name	_____
Coordinator/Director – Signature	_____

ANNEX 1: MINIMUM DATA CLASSIFICATION AND HANDLING GUIDE

Classification	Examples	Access	Minimum Handling
Public	Approved public reports, published information	General	Use approved/public versions only.
Internal	Routine internal administration and operational information	FAWS personnel with a work need	Store in approved systems; do not publish externally without authorization.
Confidential	Employee records, contracts, donor information, non-public programme information	Authorized personnel	Need-to-know access; secure storage and controlled sharing.
Sensitive	Health, financial, biometric and other legally protected sensitive information	Strictly authorized personnel	Enhanced access control, secure transmission/storage, minimum necessary disclosure and careful disposal.

ANNEX 2: INITIAL DATA RETENTION SCHEDULE TEMPLATE

The following is a governance template, not a substitute for confirming statutory, donor or contractual retention requirements. Each department should complete the final retention period before implementation.

Record Category	Purpose	Custodian	Retention Period/Criteria	Disposal Method	Approved By
Employee/personnel records	HR administration	Finance/Admin	To be confirmed against applicable law and organizational requirements	Secure destruction/deletion	_____
Payroll/financial records	Financial management and statutory/donor reporting	Finance	To be confirmed against applicable law, donor and audit requirements	Secure destruction/deletion	_____
Beneficiary/programme records	Programme implementation, M&E, reporting and accountability	Programme/M&E	To be determined per programme/donor/legal requirement	Secure destruction/deletion	_____
Procurement/supplier records	Procurement and contract management	Finance/Admin	To be confirmed against applicable law/donor requirements	Secure destruction/deletion	_____
Board/governance records	Governance and institutional memory	Board Secretariat/Coordinator	Long-term/permanent where appropriate	Secure archive	_____

ANNEX 3: DATA BREACH INITIAL RESPONSE CHECKLIST

9. Record the date/time the incident was discovered and who discovered it.
10. Notify the Data Protection Lead/Coordinator/Director immediately.
11. Identify the system, device, file or process involved.
12. Contain the incident without destroying relevant evidence.
13. Identify categories and approximate number of affected data subjects and data records.
14. Identify whether sensitive personal data is involved.

15. Assess likely consequences and risks to affected individuals.
16. Determine whether notification to the ODPC or affected individuals is required.
17. Document all decisions, actions and communications.
18. Implement corrective and preventive measures and conduct a post-incident review.

ANNEX 4: DATA SUBJECT REQUEST LOG – MINIMUM FIELDS

Request ID	Date Received	Data Subject/Identifier	Type of Request	Action/Response Date	Status

ANNEX 5: STAFF AND VOLUNTEER CONFIDENTIALITY COMMITMENT

I understand that, in the course of my duties with FAWS, I may access personal and confidential information. I undertake to use such information only for authorized FAWS purposes, protect it from unauthorized access or disclosure, follow the FAWS Data Protection Policy and promptly report any suspected loss, misuse or breach of personal data.

Name	_____
Role/Department	_____
Signature/Date	_____
Supervisor/Witness	_____