Data Protection Policy

ADOPTED POLICY

The Board of Indigenous Women Leaders of Feiyah Action Network adopted this policy at its emergency meeting on 3 November 2026, and it is in force from that date. It is reviewed every two years, and sooner if the law changes, FAN's programmes change, or a serious incident shows a weakness.

1. Why FAN has this policy

Feiyah Action Network holds personal information about children, about survivors of violence and harmful practices, and about the women and families it works with. Some of that information could put a person in danger if it reached the wrong people. In Laisamis, where communities are small and everyone is known, a leaked name carries more risk than it would in a city.

This policy sets out what FAN collects, how it is kept, who may see it, and what happens if it goes wrong. It is written to operate within the Data Protection Act 2019 of Kenya.

2. Scope

This policy applies to all personal data FAN holds, on paper, on phones, on computers and in messaging applications, and to everyone who handles it, including volunteers and consultants.

3. Definitions

Term	Meaning
Personal data	Any information that identifies a living person, or could identify them when combined with other information FAN holds.
Sensitive personal data	Data revealing health, sexual life, ethnicity, religion, marital status or family details. Much of what FAN records about FGM, child marriage and beading falls into this category.
Data subject	The person the data is about.
Data controller	The organisation deciding how and why data is used. FAN is a data controller.
Processing	Anything done with data, including collecting, recording, storing, sharing and deleting.

4. Principles

1. FAN collects only what it actually needs for a stated purpose, and no more.
2. FAN tells people what their information is for, in a language they understand, before collecting it.
3. FAN uses data only for the purpose it was collected for, unless the person agrees otherwise or the law requires it.
4. FAN keeps data accurate and corrects it when told it is wrong.
5. FAN keeps data no longer than necessary.

6. FAN keeps data secure, in proportion to the harm a leak would cause.
7. FAN can explain, at any time, what it holds and why.

5. Lawful basis and consent

- FAN relies on consent for most of its work with communities, and on contract or legal obligation for staff records.
- Consent is explained orally in Rendille, Samburu or Swahili where that is the language the person understands. A thumbprint is accepted where a person does not write.
- Consent must be a real choice. A person who declines still takes part in the activity.
- For anyone under 18, consent comes from a parent or guardian, with the child's own agreement. The consent forms in the Safeguarding and Protection Policy are used.
- Consent can be withdrawn at any time for future use.
- Sensitive personal data requires particular care and, in most cases, explicit consent. **Verify** the exact requirements for sensitive personal data under the Data Protection Act 2019 with a Kenyan advocate before adoption.

6. What FAN collects

FAN maintains a written record of what it holds, using the template at Annex A, so that it can answer a question about its data without guessing. Typical categories are:

Category	Examples and sensitivity
Participant records	Names, ages, villages, attendance. Sensitive where linked to FGM, marriage or beading work.
Safeguarding records	Concerns, referrals, outcomes. Highly sensitive. Held separately under the Safeguarding and Protection Policy.
Case stories and images	Photographs, recordings, quotations. Sensitive where the person could be identified.
Staff and volunteer records	Contracts, identification numbers, payroll, references, certificates of good conduct.
Financial records	Payment recipients, mobile money numbers, signatures.
Contact lists	Partners, officials, community representatives.

7. Keeping data safe

- Paper records containing personal data are kept in a lockable cabinet. Safeguarding records are locked separately from programme files.
- Devices holding personal data are password protected. A shared office computer has a separate account for data work.
- Personal data about children or safeguarding concerns is never sent over WhatsApp, personal email or social media.
- Attendance sheets carrying names and phone numbers are not left in a vehicle, at a venue or with a community member.
- Where data is carried into the field, only what is needed for that activity is taken.
- Backups are held by the board chairperson, and are protected to the same standard as the original. Paper backups are kept locked and digital backups are kept on a password protected device. No other board member holds a copy.

- When a staff member or volunteer leaves, their access is removed and any FAN data on a personal device is deleted, confirmed in writing.

8. Sharing data

- Personal data is shared only where there is a clear reason and, normally, consent.
- Data is shared without consent where FAN must do so to protect someone from serious harm, or where the law requires it, for example a referral to the Children's Officer or the police. This exception is explained to people before they disclose.
- Funder reports use aggregate numbers. Individual names are not sent to funders unless the funder has a lawful reason and the person agreed.
- Where data would be sent outside Kenya, for example to a funder abroad or into a cloud service hosted overseas, **verify** the conditions the Data Protection Act 2019 places on cross border transfers before sending. Do not assume that sending a spreadsheet by email is exempt.
- Partners and sub grantees receiving personal data from FAN are bound by written terms requiring equivalent protection.

9. How long FAN keeps data

Record type	Retention
Safeguarding concerns	Seven years, or until the child reaches the age of 25 where it concerns a child, whichever is later.
Participant attendance and activity records	Seven years from the end of the activity. Where a funder agreement requires longer, the longer period applies.
Consent forms	For as long as the image or story is in use, plus the period the related activity records are held.
Staff and payroll records	Seven years from the end of employment.
Financial records	Seven years, aligned with the Finance and Asset Management Policy.

At the end of the retention period, paper is shredded or burned securely and digital files are deleted from the device and the backup. Disposal of safeguarding records is recorded.

10. People's rights over their data

Under the Data Protection Act 2019, a person may ask what FAN holds about them, ask for a correction, ask for deletion, and object to certain uses. FAN does not require a written request, since many of the people FAN works with do not write.

1. A request may be made in person, by phone, or through a community representative.
2. The request is passed to the Operations and Programme Officer, who is responsible for data protection at FAN, and recorded in the log at Annex B.
3. FAN confirms the person's identity before releasing anything, taking care not to disclose data to a relative who is not entitled to it. This matters where a family member may be the source of risk.
4. FAN responds within the period the Act requires. **Verify** the statutory response period before adoption.
5. Where FAN cannot do what is asked, for example because a safeguarding record must be kept, FAN explains why.

11. If something goes wrong

A data breach means personal data lost, stolen, seen by someone who should not have seen it, or sent to the wrong person. A lost notebook of participant names is a breach. So is a photograph of an attendance sheet sent to the wrong group.

1. Tell the person responsible for data protection immediately, the same day.
2. Contain it: recover the document, ask for the message to be deleted, change the password.
3. Assess who could be harmed, and how seriously. Where the breach concerns a child or a survivor, treat it also as a safeguarding concern.
4. Record it in the breach log at Annex C, whatever its size.
5. Notify the Office of the Data Protection Commissioner where the Act requires it. **Verify** the notification threshold and the deadline, which is commonly stated as 72 hours, at odpc.go.ke before relying on any figure here.
6. Tell the people affected where they could be harmed, and tell them what to do.
7. Report every breach to the board at its next meeting.

12. Registration and responsibility

- The Data Protection Act 2019 requires certain data controllers to register with the Office of the Data Protection Commissioner. Feiyah Action Network is registered with the Office of the Data Protection Commissioner, and its certificate of registration is available on request.
- FAN names Hamed Nalle, Operations and Programme Officer, info@feiyahactionnetwork.org, as the person responsible for data protection. This is a different person from the safeguarding focal person, so that responsibility for personal data and responsibility for safeguarding concerns do not rest with one individual.
- All staff and volunteers receive a short briefing on this policy as part of induction, and annually.

13. Review

Reviewed every two years, and sooner if the law changes, FAN's systems change, or a breach reveals a weakness.

Adoption

Completed by the adopting body. The board adopted this policy at the meeting recorded below.

Field	Entry
Adopted by	The Board of Indigenous Women Leaders of Feiyah Action Network, at its emergency meeting
Date of meeting	3 November 2026
Resolution number	Min Res 6/2026
Date this version takes effect	3 November 2026
Review due	3 November 2028
Policy owner	Operations and Programme Officer
Supersedes	No previous policy. This is the first data protection policy FAN has adopted.
Date this file was issued	4 November 2026. This file was produced after the meeting, to record the decisions taken at it. The text was not altered in any other way.

Chairperson	Policy owner
Name: Signature: Date:	Name: Signature: Date:

Annex A: Record of what FAN holds

Data category	Why FAN holds it	Where it is kept	Who can see it	How long it is kept

Annex B: Log of requests from data subjects

Date received	Who asked, and how	What was asked for	Action taken	Date answered

Annex C: Breach log

Date and reference	What happened	Who could be harmed	Action taken to contain it	Reported to ODPC and board, dates