



LIVANE YOUTH FOUNDATION

DATA PRIVACY POLICY

Effective Date: August 2026

Version: 1.0

Last Updated: August 2026

1. Introduction

Livane Youth Foundation (“**Livane**”, “**we**”, “**us**” or “**our**”) is a youth-led, rights-based organisation working to advance the health, rights and socio-economic empowerment of adolescents and young people in Uganda, with current programs focused on the Sebei sub-region (Kapchorwa, Kween and Bukwo districts).

We process personal data in the course of delivering Sexual and Reproductive Health and Rights (SRHR) education, peer education, FGM prevention and alternative rites of passage work, gender-based violence (GBV) awareness, mental wellbeing support, economic empowerment activities, monitoring & evaluation, partnership engagement, and website operations.

LIVANE YOUTH FOUNDATION

This Data Privacy Policy explains:

- What personal data we collect and process
- Why and how we process it
- The legal bases we rely on
- How we protect it
- Your rights under Ugandan and international standards

This Policy is designed to comply with the **Data Protection and Privacy Act, 2019 (Cap. 97)** of Uganda and its Regulations, and aligns with internationally recognised principles of data protection (including fairness, purpose limitation, data minimisation, accuracy, storage limitation, integrity & confidentiality, and accountability).

2. Who We Are (Data Controller)

Livane Youth Foundation

Website: <https://livaneyf.org>

Email for data protection matters: **privacy@livaneyf.org** (or **info@livaneyf.org**)

Physical presence: Uganda

We act as the **Data Controller** for the personal data described in this Policy. Where we engage third-party service providers (e.g. hosting, email, monitoring tools), they act as **Data Processors** under our instructions and are required to meet equivalent protection standards.

We are committed to registering (and maintaining registration) with the **Personal Data Protection Office (PDPO)** as required under the Data Protection and Privacy Act, 2019.

3. Principles We Follow

In line with Section 3 of the Data Protection and Privacy Act, 2019, we:

1. Are **accountable** to you for personal data we collect, process, hold or use.
2. Collect and process data **fairly and lawfully**.
3. Collect, process, use or hold only data that is **adequate, relevant and not excessive**.
4. Retain personal data only for the period authorised by law or necessary for the purpose.
5. Ensure the **quality and accuracy** of information.
6. Ensure **transparency and participation** of the data subject.
7. Observe appropriate **security safeguards**.

We also apply heightened care when processing **special personal data** (including health status, medical records, sexual life or related information) that may arise in SRHR, FGM or GBV-related programme work.

4. What Personal Data We Process

Category	Examples of Data	How / When Collected	Purpose
Website & Contact Enquiries	Full name, email address, phone/WhatsApp number, organisation/role, interest area, message content	Contact form on website; email correspondence	Responding to partnership, funding, collaboration, media or general enquiries
Programme Participants (AGYW, ABYM, Peer Educators, Community Members)	Name, age/date of birth or age group, sex/gender, contact details, location (district/sub-county), school or community affiliation, attendance records, referral information	Registration forms, attendance sheets, peer education sessions, community dialogues, safe-space activities (with informed consent)	Programme delivery, peer education, referrals to youth-friendly services, safeguarding, monitoring & evaluation, reporting to partners (usually in aggregated or anonymised form)
Sensitive / Special Personal Data (processed only when strictly necessary and with explicit consent or other lawful basis)	Health-related information (e.g. SRHR service uptake indicators, HIV-related referral notes where relevant), experiences related to FGM or GBV (when disclosed for support or referral), disability status	Only during programme activities where the individual (or parent/guardian for children) has given informed consent, or where processing is necessary for medical/referral purposes consistent with the Act	Providing appropriate support, referrals, psychosocial assistance, and measuring programme outcomes while protecting dignity and confidentiality
Staff, Volunteers, Board & Peer Educators (as team members)	Name, contact details, identification documents, CV/professional background, banking details (for payments), emergency contacts	Recruitment, onboarding, contracts	Employment/volunteer management, safeguarding checks, payments, emergency contact

Partners, Funders & Collaborators	Name, organisation, email, phone, role, correspondence	Emails, partnership forms, meetings	Managing partnerships, reporting, due diligence
Website Technical Data	IP address, browser type, device information, pages visited, approximate location (city/country level), cookies	Automatically when you visit the website	Website security, performance, basic analytics, improving user experience
Photos & Media	Photographs or videos of activities (individuals may be identifiable)	Programme events and activities (with consent)	Documentation, reporting, website, social media and fundraising (only with appropriate consent)

We do not sell personal data. We do not use personal data for commercial profiling or automated decision-making that produces legal or similarly significant effects without human involvement and appropriate safeguards.

5. Legal Bases for Processing

Under the Data Protection and Privacy Act, 2019, we primarily rely on:

- **Consent** – freely given, specific, informed and unambiguous (especially for special personal data and for children, where parental/guardian consent is required).
- **Performance of a contract** or steps taken at the request of the data subject prior to entering a contract (e.g. partnership or employment).
- **Compliance with a legal obligation.**
- **Medical purposes** (where relevant to SRHR referrals and support, consistent with the Act).
- Other limited exceptions permitted by law (e.g. public duty, prevention of crime, national security) — used only when applicable and proportionate.

When we process special personal data (health, sexual life, etc.), we apply additional safeguards and obtain explicit consent unless another lawful exception clearly applies.

6. How We Use Personal Data

- Deliver youth-centred SRHR, FGM prevention, GBV awareness, mental wellbeing and economic empowerment programmes in Sebei and other areas of operation.
- Train and support peer educators.
- Make and track referrals to youth-friendly health and support services.
- Conduct monitoring, evaluation, learning and reporting (preferring aggregated or anonymised data where possible).
- Respond to enquiries from potential partners, funders, researchers and the public.
- Manage our team, volunteers and organisational operations.
- Maintain website security and functionality.
- Comply with legal, regulatory and donor requirements.
- Protect the safety and wellbeing of participants (safeguarding).

7. Sharing of Personal Data

We may share personal data only when necessary and with appropriate safeguards:

- With **service providers** (hosting, email delivery such as EmailJS/Hostinger, cloud storage) under written agreements requiring confidentiality and security.
- With **referral partners** (health facilities, psychosocial support providers) — only with consent or where necessary for the individual's care and support.
- With **funders and institutional partners** — usually in aggregated, anonymised or pseudonymised form for reporting; identifiable data only where contractually required and lawfully permitted.
- With **authorities** when required by law or to protect vital interests / prevent serious harm.
- In the event of an organisational restructuring, only subject to continued protection of the data.

We do not transfer personal data outside Uganda unless the destination country has adequate data protection measures at least equivalent to those under the Data Protection and Privacy Act, 2019, or another lawful transfer mechanism applies, and we have taken appropriate steps (including contractual clauses where required).

8. Data Retention

We retain personal data only for as long as necessary for the purposes stated or as required by law or legitimate organisational needs (e.g. donor audit periods, safeguarding records).

Typical periods (subject to review):

- Contact form enquiries: up to 2 years after last correspondence (unless a longer relationship develops).
- Programme participation records: for the duration of the programme plus a defined period for M&E, learning and accountability (commonly 3–7 years, depending on donor and legal requirements), after which data is anonymised or securely destroyed.
- Staff/volunteer records: in accordance with employment and tax law.
- Website logs: shorter periods consistent with security needs.

When retention is no longer necessary, we securely delete or irreversibly anonymise the data.

9. Security Measures

We implement technical and organisational measures appropriate to the sensitivity of the data and the risks involved, including:

- Access controls and need-to-know principles
- Secure storage (physical and digital)
- Encryption and secure transmission where appropriate
- Staff and peer educator training on confidentiality and data protection
- Confidentiality agreements
- Regular review of security practices
- Incident response procedures for suspected breaches

In the event of a personal data breach that is likely to result in a risk to rights and freedoms, we will take steps consistent with the Act and applicable guidance, including notification to the PDPO where required.

10. Your Rights

Under the Data Protection and Privacy Act, 2019, you have the right to:

- **Access** personal data we hold about you (upon providing proof of identity).
- **Request correction**, updating, blocking, erasure or destruction of inaccurate or incomplete data.
- **Object to / prevent processing** that causes or is likely to cause unwarranted substantial damage or distress.
- **Object to processing for direct marketing**.

- **Withdraw consent** at any time (where processing is based on consent), without affecting the lawfulness of processing before withdrawal.
- **Lodge a complaint** with the Personal Data Protection Office (PDPO).

To exercise any of these rights, contact us at **privacy@livaneyf.org** (or info@livaneyf.org). We will respond within the timeframes required by law (generally promptly and within 30 days where applicable).

Children and young people: Where we process data of children, we obtain prior consent of a parent or guardian as required by the Act, except where another lawful basis applies.

11. Cookies and Website Technologies

Our website may use essential cookies necessary for functionality and security, and limited analytics cookies to understand how the site is used. You can control cookies through your browser settings. We do not use cookies for invasive tracking or advertising profiles.

12. Changes to This Policy

We may update this Policy from time to time to reflect changes in our practices, programmes or legal requirements. The updated version will be posted on our website with a revised “Last Updated” date. Significant changes will be communicated through appropriate channels.

13. Contact & Complaints

Data Protection Contact

Livane Youth Foundation

Email: privacy@livaneyf.org / info@livaneyf.org

Website: <https://livaneyf.org>

Regulator

Personal Data Protection Office (PDPO)

Under the National Information Technology Authority – Uganda (NITA-U)

Website: <https://www.pdpo.go.ug> (or current official PDPO portal)

If you are not satisfied with our response, you may lodge a complaint with the PDPO.

Livane Youth Foundation is committed to protecting the dignity, privacy and rights of every young person and community member we work with. Data protection is an integral part of our rights-based, youth-led approach.