

Love Without Boundaries – Enhanced Data Privacy and Security Policy

Introduction LWB is committed to protecting privacy and ensuring the security of personal data for our donors, supporters, program participants, volunteers, team members, and partners, both in the US and internationally. We align our practices with national and international standards, including Uganda's Data Protection and Privacy Act, the EU's GDPR, and other global best practices.

Personal Data Collection

- **Data Types Collected:** We classify data into Personal Information, Non-personal Information, Usage Data, and Program Data. This includes names, addresses, program preferences, and interaction data with LWB.
- **Collection Methods:** Data is collected through our website, applications, donations, signups, and onboarding forms.
- **Lawful Basis and Transparency:** Our data collection aligns with principles of lawfulness, fairness, and transparency.

Use of Personal Data

- **Purpose:** Data is used for donation receipts, project updates, annual campaign mailings, and as necessary for the services requested by and provided to our program participants and other stakeholders.
- **Consent and Legitimate Interest:** Processing is based on explicit consent or legitimate interest.
- **Anonymized Reporting:** We use anonymized data for public reporting, respecting data source confidentiality.

Disclosure of Personal Data

- **Privacy Commitment:** We do not sell or trade personal information without prior approval.
- **Third-Party Sharing:** Data is shared with service providers for processing, referrals, care planning, and audits.



- **Data Protection Impact Assessment:** We conduct DPIAs before sharing data with third parties.

Data Security and Protection

- **Measures Adopted:** We implement strict measures, including the selection of responsible third-party vendors and service providers that utilize secure measures, including but not limited to data encryption, secure networks, and strong password policies.
- **Compliance with National and International Standards:** Our security measures comply with both national and international standards.
- **Staff Training and NDAs:** Team members undergo data security training and sign NDAs.

Data Breach Response

- **Reporting Obligations:** We follow stringent procedures for reporting data breaches in line with Uganda's Act and GDPR.

Data Retention and Rights

- **Retention Policy:** Data is retained only as long as necessary and with consent.
- **Participant Rights:** Participants have rights to access, correct, or request data deletion.

International Considerations

- **Cross-Border Data Transfers:** We work to ensure compliance with international data protection laws for cross-border transfers.

Handling of Personal and Sensitive Information

- **Necessity for Services:** We acknowledge the importance of personal and sensitive data, including medical data, for service provision.



- **Special Categories of Data:** Additional safeguards are applied for processing special categories of personal data.
- **Handling of Minors' Data:** We collect minors' data only with explicit parental or guardian consent.

Parental/Guardian Consent and Rights

- **Informed Consent Process:** We engage in a comprehensive consent process with parents or guardians before collecting minors' information.
- **Rights of Parents/Guardians:** Parents or guardians can review, amend, or request deletion of their child's information.

Accountability and Governance

- **Regular Audits and Reviews:** Our practices are regularly audited to ensure compliance with evolving laws and standards.
- **Data Protection Training:** Staff receive regular training in handling personal and sensitive data.

Contact and Feedback

- **Transparent Communication:** Stakeholders are encouraged to contact us at info@lwmail.com for any inquiries or feedback.

Policy Review and Updates

- **Dynamic Compliance:** This policy will be dynamically updated to reflect changes in data protection laws and best practices.

This policy ensures LWB's dedication to ethical practices, legal compliance, and the provision of high-quality, respectful services, while addressing the unique needs associated with handling personal and sensitive information.

Approved January 2024

