Anti-Money Laundering & Countering the Financing of Terrorism (AML/CFT) Policy & Procedures Manual

Open World Foundation (OWF)

Document Control

Policy Title: Anti-Money Laundering and Countering the Financing of Terrorism Policy & Procedures Manual

Version: 1.0 (Draft for NGO use – Voluntary / Best Practice)

Effective Date: April 2026

Review Frequency: Annually or upon material change

Approved by: Board of Directors / Executive Director

Disclaimer

This Manual is designed to assist Open World Foundation in implementing best practices related to Anti-Money Laundering and Countering the Financing of Terrorism but is not intended to be a substitute for the respective laws and Regulations on the same. Furthermore, the Foundation should utilize the Manual in light of its professional judgment and the facts and circumstances involved in its operations and each particular donor or partner relationship. The Foundation is encouraged to develop and customize its own manual for the execution of its role. OWF disclaims any responsibility or liability that may occur, directly or indirectly, as a consequence of the use and application of the Manual.

Table of Contents

Table of Contents

1.0 General Policy Statement 5
2.0 Anti-Money Laundering & Countering Terrorist Financing (AML/CFT) Policies, Controls and Procedures 5
3.0 Policy and Procedure Regarding the Anti Money Laundering Compliance Lead 6
4.0 Policy and Procedure for AML Training Program for Staff 7
5.0 Policy and Procedure for Donor/Partner Identification 8
6.0 Donor/Partner Identification Procedures for Natural Persons 10
7.0 Procedures for Corporations, Partnerships, Trusts and Other Legal Entities 10
The organization shall follow identification requirements as prescribed by the Regulations to establish the identity of foreign nationals, entities and local entities and other bodies. 11
8.0 Policy and Procedure for Money Laundering Risk Assessment 11
9.0 Donor/Partner Identification Procedures for 'High-Risk' Natural Persons 12
10.0 Policy and Procedure for Knowing the Donor's/Partner's Business as Part of Due Diligence (DD) 12
11.0 Policy and Procedure for Internal Reporting of Suspicious Transactions 14
12.0 Policy and Procedure for Ongoing Monitoring of Activities 15
13.0 Policy and Procedure for Keeping Records of Due Diligence Information 16
Policy 16
14.0 Policy and Procedure for Formal Disclosures to the Authorities 17
15.0 Policy and Procedure for Stopping/Continuing Work Following a Suspicion Report 18
15.3 On receipt of a suspicion report, the Compliance Lead shall: 19
16.0 Policy and Procedure for the Monitoring and Management of Compliance 19
Policy 19
17.0 Policy and Procedure for Review of the Manual 20
Policy 20

Acronyms Used in the Manual

AML: Anti-Money Laundering

CFT: Counter Terrorist Financing MLCO:

Money Laundering Control Officer (referred to as Compliance Lead in this NGO context)

KYC: Know Your Customer (adapted to Know Your Donor/Partner)

FATF: Financial Action Task Force

DD: Due Diligence

EDD: Enhanced Due Diligence

.

1.0 General Policy Statement

Open World Foundation is committed to full compliance with all applicable laws and regulations regarding Money Laundering and Terrorist Financing, even on a voluntary basis. OWF has adopted and will enforce the provisions set forth in this Anti-Money Laundering & Counter Terrorist Financing Policy and Procedures Manual in order to prevent and detect money laundering, terrorist financing and other illegal activities. The Board and Management of OWF consider Integrity as a key commitment on the part of the organization to uphold strict standards of ethical conduct and hence preservation of a stable value for society confidence. These policies endorse the strict compliance with the legal framework governing the prevention of money laundering and terrorism financing.

The organization's commitment to this objective is set forth in this Policy which defines the guiding policies for adequate prevention and control. It includes procedures for the detection and reporting of activities possibly linked to money laundering or the financing of terrorist activities.

If OWF and/or its personnel are inadvertently used for money laundering or other illegal activities, OWF can be subject to potentially serious civil and/or criminal penalties. Therefore, the appropriate application of the Policy requires that staff of the organization be familiar with the contents herein, related procedures and norms that regulate the various activities and services of the organization as compliance with the provisions is compulsory to all the organization's staff.

2.0 Anti-Money Laundering & Countering Terrorist Financing (AML/CFT) Policies, Controls and Procedures

Policy Statement

It is the policy of OWF that all members of staff at all levels actively participate in preventing the services of the organization from being exploited by criminals and terrorists for money laundering purposes. This participation has its objectives as:

- Complying with all Anti-Money Laundering Act & Regulations of the jurisdictions
- Requiring all Employees to prevent, detect and report to the Compliance Lead all potential instances in which OWF or its Employees, its facilities or its activities have been or are about to be used for money laundering, terrorist financing and other illegal activity;
- Providing for a Compliance Lead who shall ensure adherence to the OWF's AML & CFT Policies and Procedures;
- Requiring all appropriate employees to attend anti-money laundering training sessions, so that all employees are aware of their responsibilities under OWF's policies and procedures; these Guidelines and as affected by current developments with respect to anti-money laundering legislations.

- Protecting the organization and all its staff as individuals from the risks associated with breaches of the law, regulations and supervisory requirements.
- Preserving the good name of the organization against the risk of reputational damage presented by implication in money laundering and terrorist financing activities.

It shall be the policy of this organization that:

- Every member of staff shall meet their personal obligations as appropriate to their role and position in the organization.
- Neither commercial considerations nor a sense of loyalty to donors/partners shall be permitted to take precedence over the organization's anti-money laundering commitment.
- The organization shall carry out a business-wide assessment of the risks of money laundering and terrorist financing to which the organization is subject and design and implement appropriate controls to mitigate and manage effectively the risks identified.
- The organization shall establish and maintain documented, proportionate policies and procedures, including controls, which outline the positive actions to be taken by staff to prevent money laundering and terrorist financing in the course of their work.

3.0 Policy and Procedure Regarding the Anti Money Laundering Compliance Lead

Policy

It is the policy of the organization that a Compliance Lead shall be appointed and this shall be a person in a senior managerial position, possessing sufficient professional experience and competence. The organization shall notify the appointment of such a person or their cessation to the NGO Bureau if required.

For avoidance of doubt, in this manual, the 'Authority' means the Financial Intelligence Authority, while the NGO Bureau means the Uganda National NGO Bureau.

Procedures

3.1 The organization shall appoint a senior manager as the Compliance Lead who shall from time to time coordinate AML activities and compliance responsibilities.

3.2 Any staff shall immediately notify the Compliance Lead if he/she suspects or has any reason to suspect that any potentially suspicious activity has occurred or will occur if a transaction is completed.

3.3 Staff are encouraged to seek the assistance of the Compliance Lead with any questions or concerns they may have with respect to the OWF's Anti-Money Laundering Policies or Procedures.

3.4 Responsibilities of the Compliance Lead include the following:

- Coordination and monitoring of OWF's day-to-day compliance with applicable Anti-Money Laundering Laws and Regulations and OWF's own Anti-Money Laundering Policy and Procedures;
- Develop and implement systems, mechanisms and procedures to ensure that the staff of the organization report any suspicious money laundering or financing of terrorism activity;
- Conduct staff training programs for appropriate personnel related to the OWF's anti-money laundering policy and procedures and maintaining records evidencing such training;
- Receive and review any reports of suspicious activity from staff;
- Coordination of enhanced due diligence procedures regarding donors/partners and respond to both internal and external inquiries regarding OWF's AML/CFT policies and procedures.
- Notify the Authority of any suspicious money laundering or financing of terrorism activity, if deemed necessary under voluntary best practices.

4.0 Policy and Procedure for AML Training Program for Staff

Policy

It is the policy of OWF that recruitment of all staff will include adequate screening procedures to ensure high standards when hiring staff.

It is the policy of OWF that all staff who have donor/partner contact, or access to information about donors'/partners' affairs, shall receive AML/CFT training to ensure that their knowledge and understanding is at an appropriate level, and ongoing training at least annually to maintain awareness shall be ensured.

It is the policy of OWF that all staff who have donor/partner contact, or access to personal data relating to donors/partners, shall receive training on the law relating to data protection to ensure that their knowledge and understanding is at an appropriate level, and ongoing training at least annually to maintain awareness and ensure that the organization's legal obligations are met.

It is the policy of the organization that all staff are required to reconfirm their awareness of the contents of this Compliance Manual by signing the acknowledgement form annually, or more frequently, as required by the Compliance Lead.

The Compliance Lead shall ensure that training is made available to staff according to their exposure to money laundering risk, and that steps are taken to check and record that training has been undertaken and that staff have achieved an appropriate level of knowledge and understanding.

Procedure

4.1 All staff are required:

- At a time specified by the Compliance Lead, to undertake training programs on anti-money laundering policies and procedures.
- To get trained in how to recognize and deal with transactions which may be related to money laundering.
- To timely escalate and report the matter to the Compliance Lead.
- To get themselves acquainted and comply with Anti Money Laundering Act & Regulations.

4.2 The Compliance Lead will evaluate alternative AML/CFT training methods, products and services in order to make suitable training activities available to all members of staff who have donor/partner contact, or access to information about donors'/partners' affairs.

4.3 The training programme will include means of confirming that each individual has achieved an appropriate level of knowledge and understanding, whether through formal testing, assessment via informal discussion, or other means.

4.4 The Compliance Lead will keep records of training completed, including the results of tests or other evaluations demonstrating that each individual has achieved an appropriate level of competence.

4.5 The Compliance Lead will assess the effectiveness of the programme completed and update the training information to match with the changes in laws, regulations, guidance and practice as a way of considering relevant continuity of the training programme.

5.0 Policy and Procedure for Donor/Partner Identification

Policy

It is the policy of OWF's anti-money laundering policies and procedures that, prior to accepting funds from donors or entering partnerships, all reasonable and practical measures are taken to confirm the donors'/partners' identities and to verify that any third party upon whom OWF relies for identification, such as a bank and other financial intermediary, or any other third party adheres to the same standards.

General Procedure

5.1 These Donor/Partner Identification Procedures are based on the premise that the OWF will accept funds from a new and existing donor/partner only after:

- OWF has confirmed the donor's/partner's identity and that the donor/partner is acting as a principal and not for the benefit of any third party unless specific disclosure to that effect is made; or

- If the donor/partner is acting on behalf of others, OWF has confirmed the identities of the underlying third parties.

5.2 The Donor/Partner Identification Procedures should be reviewed in light of the specific characteristics presented by a donor/partner and in any instance the Compliance Lead may determine to apply Enhanced Due Diligence (EDD) measures for any other justifiable reasons.

5.3 As a reference tool, an Individual Donor/Partner KYC Checklist is used. Staff is encouraged to provide the Compliance Lead with any revisions they consider appropriate.

5.4 The Compliance Lead shall retain copies of all documents reviewed or checklists completed in connection with its Donor/Partner Identification Procedures in accordance with OWF's Records Retention policies.

5.5 The member of staff conducting verification of identity will complete the process by checking that the donor/partner is not the subject of sanctions or other statutory measures, using the screening methods set out by the Compliance Lead.

5.6 The organization's Compliance Lead will maintain a list of acceptable documents or information obtained from a reliable source which is independent of the donor/partner.

5.7 In cases where a donor/partner cannot produce acceptable documents, the responsible staff will make a risk-based decision on accepting the documents that are available, consulting with the Compliance Lead if appropriate.

5.8 Where the donor/partner is not the beneficial owner of assets involved, the responsible staff will take the necessary steps to determine who the beneficial owner is, and take reasonable measures to verify their identity accordingly.

5.9 The Compliance Lead will prepare a format for use by the responsible staff in requesting verification of identity and beneficial ownership information from relevant corporate entities and trustees, and a procedure for following up when requests are not met within the statutory period.

5.10 If all possible means of identifying the beneficial owner of a donor/partner entity have been exhausted without success, and recorded, the responsible staff will seek the approval of the Compliance Lead, to be given on a risk-sensitive basis, to treat as its beneficial owner the natural person who exercises ultimate effective control over the donor/partner entity.

5.11 In all cases assessed as presenting a higher money laundering risk, where enhanced due diligence is required, the Compliance Lead will consult with the Executive Director to decide on additional steps to verify the donor's/partner's identity.

5.12 All verification of identity processes as well as actions taken to verify the identity of corporate entities will be recorded. This will include keeping photocopies of documents produced, or in exceptional cases with the approval of the Executive Director, recording information about where copies are held and can be obtained.

6.0 Donor/Partner Identification Procedures for Natural Persons

6.1 OWF shall take reasonable steps to ascertain satisfactory evidence of an individual donor's/partner's name, details of the residential address, the telephone contact including the mobile telephone, e-mail address, date and the source of the donor's/partner's funds. 6.2 In order to confirm the identity of the donor/partner, copies of the following documents will be obtained and retained for OWF's records:

- the donor's/partner's national identification card or an alien's identification card, whichever is applicable;
- an introductory letter from the employer or a senior government official attesting to the identity of the person;
- in the case of a student, an introductory letter from the school and a copy of the student's identity card;
- a summary of the nature of business activities the person is engaged in; 6.3 Additional information which may be requested for includes:
- utility bills including electricity and water bills;
- details on occupation or employment;
- details of source of income;
- income tax identification number, where applicable

7.0 Procedures for Corporations, Partnerships, Trusts and Other Legal Entities

OWF shall take reasonable steps to ascertain satisfactory evidence of an entity donor's/partner's name and address, its authority to make the contemplated donation or partnership.

OWF will obtain certainty of the following, as appropriate under the circumstances:

- the name of the entity, and where applicable its registered name and registration number;
- a copy of the deed;
- details of the registered address or principal place of business or office;
- the names, date and place of birth, identity card number or passport number, tax identification number and address of persons managing the entity;
- the financial statements of the immediate last year in case of partnerships and
- the full name of the trustee, beneficiaries or any other natural person exercising control over the trust; and the founder or sponsor of the trust in case of a trust

Where the donor/partner is a corporate entity such as a private limited company, the responsible staff will check that the entity is appropriately incorporated and registered,

and take the necessary steps to determine who are the principal beneficial owners, and the people with significant control, and their identity will be verified according to this procedure.

The organization shall follow identification requirements as prescribed by the Regulations to establish the identity of foreign nationals, entities and local entities and other bodies.

8.0 Policy and Procedure for Money Laundering Risk Assessment

Policy

It is the policy of the organization to identify and assess the money laundering and terrorist financing risks represented by the activities the organization conducts so that the organization can mitigate that risk by applying appropriate levels of due diligence.

It is the policy of the organization that the Compliance Lead will from time to time update a list of the types of donors/partners that the organization considers to be of 'high risk,' such that enhanced due diligence procedures are warranted compared to the routine identification procedures.

Procedures

8.1 The organization shall assess the money laundering risk represented by our donors/partners and the activities conducted according to three levels:

- the range normally dealt with by the organization, requiring the organization's normal level of due diligence
- an exceptionally high level of risk requiring an enhanced level of due diligence
- a negligible level of risk requiring only simplified or reduced due diligence measures. Appendix I demonstrates the risk rating for the organization

8.2 The organization shall identify and maintain lists of risk factors (including those required by the Regulations) relating to our donors/partners, programs or services, transactions, delivery channels and geographic areas of operation. 8.3 The organization shall update the risk assessment annually to ensure new and emerging risks are addressed, and new information supplied by our regulatory authority is reflected. 8.4 The money laundering or terrorist financing risk represented by each donor/partner will be assessed:

- during the new donor/partner acceptance process and/or during continuance process for continuing donors/partners;
- whenever the organization's process of ongoing monitoring indicates that a change in the activities or operating environment of an established donor/partner may represent a change in money laundering risk. 8.5 Donor/partner risk assessment shall be carried out by the responsible staff

who will determine appropriate due diligence measures in respect of each donor/partner based on:

- the organization's business-wide risk assessment
- assessment of the level of risk arising in any particular case. 8.6 A record must be made of the assessment of individual donor/partner relationships, confirming that the organization's business-wide risk assessment has been taken into account, and any other relevant factors considered. 8.7 The following are the examples of donors/partners who pose a high money laundering risk:
- A Political figure, any member of a Political Figure's Immediate Family, and any Close Associate of a Senior Political Figure;
- Any donor/partner resident in, or organized or incorporated under the laws of, a Non-Cooperative Jurisdiction; and/or high risk countries.
- Any donor/partner who gives the Compliance Lead any reason to believe that its funds originate from, or are routed through, an account maintained at an "offshore bank", or a bank organized or chartered under the laws of a Non-Cooperative Jurisdiction; and
- Any donor/partner who gives the Compliance Lead any reason to believe that the source of its funds may not be legitimate or may aid terrorist activities.

9.0 Donor/Partner Identification Procedures for 'High-Risk' Natural Persons

9.1 Enhanced Donor/Partner Identification Procedures shall be conducted for 'high risk' natural persons and such procedures shall include, but are not limited to, the following:

- Assessing the donor's/partner's reputation through review of financial or professional references, generally available media reports or by other means;
- Considering the source of the donor's/partner's wealth, including the economic activities that generated the donor's/partner's wealth and the source of the particular funds intended to be used to make the donation;
- Reviewing generally available public information, such as media reports, to determine whether the donor/partner has been the subject of any criminal or civil enforcement action based on violations of anti-money laundering laws or regulations or any investigation, indictment, conviction or civil enforcement action relating to financing of terrorists;

9.2 The enhanced due diligence procedures undertaken with respect to 'high risk' donors/partners must be thoroughly documented in writing, and any questions or concerns with regard to a 'high risk'

10.0 Policy and Procedure for Knowing the Donor's/Partner's Business as Part of Due Diligence (DD)

Policy

It is the policy of this organization to obtain information enabling us to assess the purpose and intended nature of every donor's/partner's relationship with the organization.

It is the policy of the organization to keep any information obtained during a DD for a minimum period of five years from the date the relevant business or transaction is completed with the donor/partner.

It is the policy of this organization not to offer its services, or to withdraw from providing its services, if a satisfactory understanding of the nature and purpose of the donor's/partner's business with us cannot be achieved.

Procedures

10.1 The responsible staff will obtain Know Your Donor's/Partner's business information from donors/partners:

- on acceptance of a new donor/partner
- on receipt of a new instruction from a donor/partner whose arrangements are of a one-off nature
- on any significant change in the donor's/partner's arrangements such as the size or frequency of transactions, nature of activities conducted, involvement of new parties or jurisdictions
- as an ongoing exercise throughout the donor/partner relationship.

10.2 Know Your Donor's/Partner's information sought from donors/partners will include, but not be limited to:

- the donor's/partner's reason for choosing this organization
- the purpose and justification behind the donations/partnerships the donor/partner is asking the organization to provide
- the provenance of funds introduced or assets involved in the donor's/partner's arrangements
- the nature, size, frequency, source and destination of anticipated transactions
- the counter-parties and jurisdictions concerned.

10.3 The information will be obtained by interview between the organization's staff and the donor's/partner's representative and this information shall be recorded on the donor/partner file, to assist with future monitoring of the relationship.

10.4 The information volunteered by the donor/partner shall be corroborated for consistence with any publicly accessible information to the best extent possible.

10.5 Where answers given by the donor/partner are implausible, or inconsistent with other information, or where the donor/partner is unwilling to provide satisfactory answers to due diligence enquiries, the responsible staff will consider whether the organization should withdraw from the relationship.

11.0 Policy and Procedure for Internal Reporting of Suspicious Transactions

Policy

It is the policy of this organization that every member of staff shall remain alert for the possibility of money laundering, and shall pay attention to and report all complex, unusual or large transactions, whether completed or not, and to all unusual patterns of transaction which have no apparent economic or lawful purpose and every suspicion for which they believe there are reasonable grounds, following the organization's procedure.

It is the policy of the organization that every member of staff shall pay attention to and report to the Compliance Lead:

- any transactions made on behalf of a person whose identity has not been established;
- business relations and transactions with persons in jurisdictions that do not have adequate systems to prevent or deter money laundering or the financing of terrorism; and
- electronic funds transfers that do not contain complete originator information.

The expectation placed on each individual member of staff in responding to possible suspicions shall be appropriate to their position in the organization.

Procedures

11.1 Every member of staff must be alert for the possibility that the organization's services could be used for money laundering purposes, or that in the course of their work they could become aware of criminal or terrorist property.

11.2 A member of staff becoming aware of a possible suspicion shall gather relevant information that is routinely available to them and decide whether there are reasonable grounds to suspect money laundering. Any additional DD information acquired, in particular any explanations for unusual instructions or transactions, should be recorded on the donor/partner file in the routine manner, but no mention of suspected money laundering is to be recorded in any donor/partner file.

11.3 The requirement to gather relevant information does not extend to undertaking research or investigation, beyond using information sources readily available within the organization.

11.4 If after gathering and considering routinely available information, the member of staff is entirely satisfied that reasonable grounds for suspicion are not present, no further action should be taken otherwise where there reasonable grounds for suspicion, the staff shall raise the matter with the Compliance Lead.

11.5 Where a member of staff based on their own observations decides that there are reasonable grounds to suspect money laundering, he or she shall submit a suspicion report to the Compliance Lead, in the format specified by the Compliance Lead for that purpose. Such internal suspicion report does not breach donor/partner confidentiality.

11.6 A member of staff who forms or is aware of a suspicion of money laundering shall not discuss it with any outside party, or any other member of staff unless directly involved in the matter causing suspicion.

11.7 No member of staff shall at any time disclose a money laundering suspicion to the person suspected, whether or not a donor/partner, or to any outside party. If circumstances arise that may cause difficulties with donor/partner contact, the member of staff must seek and follow the instructions of the Compliance Lead.

12.0 Policy and Procedure for Ongoing Monitoring of Activities

Policy

It is the policy of this organization to put in place policies, controls and procedures for monitoring the implementation of policies, controls and procedures to address the risks relating to money laundering and terrorism financing, and where necessary, enhance them on a regular basis.

It is the policy of the organization to maintain a system of regular, independent reviews to understand the adequacy and effectiveness of the Money Laundering and Terrorist Financing systems and any weaknesses identified.

It is the policy of this organization to monitor donors'/partners' instructions and transactions to ensure consistency with those anticipated and with the risk profile.

Procedures

12.1 All staff will maintain alertness for donors'/partners' instructions and transactions which represent a significant divergence from those anticipated for the donor/partner and feedback shall be communicated to the Compliance Lead.

12.2 The organization shall employ a suitable mechanism for monitoring donors'/partners' transactions, according to their number and the involvement or otherwise of members of staff in their execution.

12.3 Where a donor's/partner's instruction or transaction is not consistent with what is anticipated: an explanation will be sought, if appropriate by contacting the donor/partner.

12.4 The involvement of unexpected jurisdictions or organization will be checked with the organization's Compliance Lead for possible alerts or sanctions

- if a satisfactory explanation is found, the donor/partner file will be updated to record that explanation and to reflect the change in anticipated activities
- if no satisfactory explanation is found, the matter will be brought to the attention of the Compliance Lead, who will consider whether there are grounds to suspect money laundering 12.5 The Compliance Lead will consider whether there is cause to carry out a re-assessment of money laundering risk, and if so, will carry this out.

12.6 Irrespective of whether specific incidents have caused a re-assessment of money laundering risk, every donor/partner file will be reviewed periodically to check that:

- the information held is still adequate, correct and up to date
- the level of due diligence being applied is still appropriate.

12.7 Periodic review of donor/partner files will be conducted at the following intervals:

- for high-risk donors/partners – every six months
- for all other donors/partners – annually.

12.8 As part of their improvement efforts the organization shall monitor publicly-available information on best practice in dealing with Money Laundering and Terrorist Financing risks.

13.0 Policy and Procedure for Keeping Records of Due Diligence Information

Policy

It is the policy of this organization to establish and maintain systems to keep records of enquiries made and information obtained while exercising due diligence for AML purposes, and to ensure that these records are retrievable as required for legal and regulatory stipulations.

It is the policy of this organization to ensure that principles of due diligence are adhered to at the start of a new business relationship; at appropriate points during the lifetime of the relationship and when an occasional transaction is to be undertaken.

Procedures

13.1 When information is being collected for AML due diligence, the responsible staff will ensure that:

- information collected is recorded in a consistent manner in the donor/partner file, or other appropriate place.
- all instances are recorded where information requested has not been forthcoming, or where explanations provided have not been satisfactory.

13.2 The organization shall have systems to routinely archive DD records along with the organization's accounting records to ensure their availability for a minimum of ten years from the date of the completion of the transaction or enquiry.

13.3 The organization shall have data retrieval systems which facilitate full and rapid retrieval of all relevant DD records by authorised staff, in order to respond fully to enquiries from financial investigators.

13.4 The organization shall have procedures to ensure that any personal data obtained for DD purposes is processed only for the purposes of preventing money laundering and terrorist financing.

13.5 The organization shall provide new donors/partners with the statement prior to establishing a business relationship that any personal data received from the donor/partner will be processed only for the purposes of preventing money laundering and terrorist financing. 13.6 The organization shall have a procedure to earmark relevant personal data for deletion at the end of the ten year retention period unless:

- it is required for court proceedings
- the data subject has given express consent to the retention of that data.

13.7 For donors/partners who have been the subject of a suspicion, relevant records will be retained separately from the organization's routine archives, and not destroyed, even after the ten year period has elapsed, without confirmation from the Compliance Lead that they are no longer required as part of an enquiry.

13.8 In recording and documenting money laundering suspicion reports, the Compliance Lead shall at all times protect the organization's position with regard to the Data Protection Act, 2019.

14.0 Policy and Procedure for Formal Disclosures to the Authorities

Policy

It is the policy of this organization that the Compliance Lead shall receive and evaluate internal suspicion reports, and decide whether a formal disclosure is to be made to the authorities. If so deciding, the Compliance Lead will make the formal disclosure on behalf of the organization, using the appropriate mechanism.

Procedures

14.1 On receipt of a money laundering suspicion report from a member of staff, the Compliance Lead shall acknowledge its receipt in writing, referring to the report by its date and unique file number, without including the name of the person(s) suspected. This confirms to the member of staff that their legal obligation to report has been fulfilled.

14.2 The Compliance Lead shall open and maintain a log of the progress of the report. This log shall be held securely and shall not form part of the donor/partner file.

14.3 Following receipt of a report, the Compliance Lead shall gather all relevant information held within the organization, and make all appropriate enquiries of members of staff anywhere in the organization, in order properly to evaluate the report. The Compliance Lead shall then decide whether they personally believe there are reasonable grounds for suspicion, and make a decision on the organization's obligation to make a formal disclosure to the authorities.

14.4 All members of staff, anywhere in the organization, shall respond in full to all enquiries made by the Compliance Lead for the purposes of evaluating a suspicion report. Information provided to the Compliance Lead in response to such enquiries does not breach donor/partner confidentiality/professional privilege, and no member of staff shall withhold information on those grounds.

14.5 If deciding that a formal disclosure to the authorities is required, the Compliance Lead shall make such disclosure by the appropriate means.

14.6 The Compliance Lead shall document in the report log the reasons for deciding to make or not to make a formal disclosure.

14.7 The Compliance Lead shall where appropriate inform the originator of the internal report whether or not a formal disclosure has been made.

14.8 The Compliance Lead shall inform all those, and only those, members of staff who need to be aware of the suspicion in order to protect them and the organization from possible money laundering offences in connection with any related activities.

14.9 Following a formal disclosure, the Compliance Lead shall take such actions as required by the authorities in connection with the disclosure.

15.0 Policy and Procedure for Stopping/Continuing Work Following a Suspicion Report

Policy

It is the policy of this organization that from the moment a suspicion of money laundering arises, no further work will be carried out on the matter that gave rise to the suspicion. Neither commercial considerations nor the difficulty in responding to the donor's/partner's enquiries on the matter shall be permitted to take precedence over the organization's legal obligations in this regard.

In such circumstances the Compliance Lead shall act with all possible speed to enable work to continue, or if appropriate to withdraw from the donor/partner relationship, and assist staff in any communications with the donor/partner affected.

Procedures

15.1 As soon as a member of staff forms or becomes aware of a suspicion of money laundering, no further work is to be done on the matter giving rise to suspicion.

15.2 If there is any likelihood of the donor/partner becoming aware that work has stopped, for example because an anticipated transaction has not gone through, the member of staff concerned must contact the Compliance Lead for instructions on how to handle the matter with the donor/partner.

15.3 On receipt of a suspicion report, the Compliance Lead shall:

- instruct the originator of the report and any other staff involved to cease work on the matter giving rise to suspicion
- decide in the shortest possible time whether all work for the donor/partner concerned should be stopped, or whether other work that is not the cause of suspicion may continue, and advise relevant staff accordingly
- assist all affected staff in handling the matter with the donor/partner so that no tipping off offence is committed.

15.4 When work for a donor/partner has been stopped, the Compliance Lead shall carry out the evaluation of the suspicion report as quickly as possible to decide whether a disclosure must be made to the authorities or not.

16.0 Policy and Procedure for the Monitoring and Management of Compliance

Policy

It is the policy of this organization to monitor our compliance AML/CFT with legal and regulatory requirements and conduct an annual independent AML/CFT compliance audit, the findings of which are to be considered and appropriate recommendations for action set out.

The organization's Board shall provide the necessary authority and resources for the ongoing implementation of a compliant AML regime.

Procedures

16.1 The Compliance Lead will monitor continuously all aspects of the organization's AML/CFT policies and procedures, together with changes and developments in the legal and regulatory environment which might impact the organization's business-wide risk assessment.

16.2 Any deficiencies in AML/CFT compliance requiring urgent rectification will be dealt with immediately by the Compliance Lead, who will report such incidents to the organization's Board when appropriate and request any support that may be required.

16.3 The Compliance Lead will facilitate and assist the NGO Bureau review team when conducting inspections on the organization, if applicable.

17.0 Policy and Procedure for Review of the Manual

Policy

It is the policy of this organization to review the manual to keep it updated with the amendments in laws and regulations and also accommodate best practices

Procedure

17.1 A regular review of the program should be undertaken to ensure that it is functioning as designed. Such a review could be performed by external or internal resources, and should be accompanied by a formal assessment or written report. 17.2 If and when regulations are amended concerning reporting of suspicious activities, the organization will amend this Manual to comply with those regulations.

Appendix I: Risk Factors

High risk factors

Customer (Donor/Partner) risk factors, including whether;

(a) the relationship is conducted in unusual circumstances;
(b) the donor/partner is resident in a geographical area of high risk (see below);
(c) the donor/partner is a legal person or legal arrangement that is a vehicle for holding personal assets;
(d) the donor/partner is a company that has nominee shareholders or shares in bearer form;
(e) the donor/partner is a business that is cash intensive;
(f) the corporate structure of the donor/partner is unusual or excessively complex given the nature of the company's business;

Product, service, transaction or delivery channel risk factors, including whether;

(a) the program involves private banking;
(b) the program or transaction is one which might favour anonymity;
(c) the situation involves non-face-to-face relationships or transactions, without certain safeguards, such as electronic signatures;
(d) payments will be received from unknown or unassociated third parties;
(e) new programs and new practices are involved, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing programs;
(f) the service involves the provision of nominee directors, nominee shareholders or shadow directors, or the formation of companies in a third country;

Geographical risk factors, including;

(a) countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective systems to counter money laundering or terrorist financing;
(b) countries identified by credible sources as having significant levels of corruption or other criminal activity, such as terrorism, money laundering, and the production and supply of illicit drugs;
(c) countries subject to sanctions, embargos or similar measures issued by, for example, the African Union, European Union or the United Nations;
(d) countries providing funding or support for terrorism;
(e) countries that have organisations operating within their territory which have been designated by the government of Uganda as proscribed organisations under the second Schedule to the Anti-Terrorism Act 2002;
(f) countries identified by credible sources, such as evaluations, detailed assessment reports or published follow-up reports published by the Financial Action Task Force, the International Monetary Fund, the World Bank, the Organisation for Economic Co-operation and Development or other international bodies or non-governmental organisations as not implementing requirements to counter money laundering and terrorist financing that are consistent with the recommendations published by the Financial Action Task Force in February 2012 and updated in October 2016.

Low risk factors

Customer (Donor/Partner) risk factors, including whether the donor/partner;

(a) is a public administration, or a publicly owned enterprise;
(b) is an individual resident in a geographical area of lower risk (see sub section below);
(c) is an institution required to oblige by provisions of the AML Act;
(d) is a company whose securities are listed on a regulated market, and the location of the regulated market;

Product, service, transaction or delivery channel risk factors, including whether the product or service is;

(a) a life insurance policy for which the premium is low;
(b) an insurance policy for a pension scheme which does not provide for an early surrender option, and cannot be used as collateral;
(c) a pension, superannuation or similar scheme which satisfies the following conditions:

- the scheme provides retirement benefits to employees;
- contributions to the scheme are made by way of deductions from wages; and
- the scheme rules do not permit the assignment of a member's interest under the scheme;

Geographical risk factors, including whether the country where the donor/partner is resident, established or registered or in which it operates is;

(a) an EAC member state;
(b) a third country which has effective systems to counter money laundering and terrorist financing;
(c) a third country identified by credible sources as having a low level of corruption or other criminal activity, such as terrorism, money laundering, and the production and supply of illicit drugs;
(d) a third country which, on the basis of credible sources, such as evaluations, detailed assessment reports or published follow-up reports published by the Financial Action Task Force, the International Monetary Fund, the World Bank, the Organisation for Economic Co-operation and Development or other international bodies or nongovernmental organisations:

- has requirements to counter money laundering and terrorist financing that are consistent with the revised Recommendations published by the Financial Action Task Force in February 2012 and updated in October 2016; and
- effectively implements those Recommendations.

Approval This policy is approved by: [Name & Signature – Board Chair / Executive Director] [Date]