Anti-Money Laundering (AML) Policy and Counter-Terrorism Financing (CTF) Policy

1. INTRODUCTION

Catholic Family Life Limited and CFL Lumens Trust, collectively known as Catholic Family Life ("CFL") is committed to detecting and preventing occurrences of money laundering activities and the financing of terrorism in connection with its operations. To this end, CFL is committed to complying with all applicable Singapore laws and regulations that are in force to combat such money laundering activities and the financing of terrorism in Singapore, including the provisions under (i) the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 ("CDSA"); and (ii) the Terrorism (Suppression of Financing) Act 2002 ("TSOFA").

2. SCOPE

This Anti-Money Laundering Policy ("AML") and Counter-Terrorism Financing ("CTF") policy (this "Policy") is intended to outline CFL's internal framework to safeguard against potential abuse related to money laundering or terrorist activities. This policy applies to all CFL personnel, including trustees, directors, volunteers and employees. It is the responsibility of everyone involved with CFL to be familiar with and comply with this policy, and robustly protect themselves and CFL against the risks of money laundering or terrorist financing activities.

3. DEFINITION OF MONEY LAUNDERING AND FINANCING OF TERRORISM

3.1. **"Money laundering**" refers to the process by which criminals attempt to re-integrate the proceeds of their criminal activities (e.g. from drug trafficking or other criminal activities) into the financial system in an attempt to obscure the link between the funds and the original criminal activity.

a) Generally, money laundering comprises three (3) stages:

- **i.** **Placement**: This is the physical or financial disposal of the benefits derived from criminal activity and/or conduct.
- **ii.** **Layering**: This is the process of separating the benefits from their original source by creating layers of financial transfers designed to disguise the ultimate source and the audit trail.
- iii. **Integration**: This is the provision of apparent legitimacy to the benefits derived from criminal activity and/or conduct. If the layering process is successful, the integration scheme(s) places the laundered funds back into the economy so that these funds re-enter the financial system, appearing to be legitimate fund. Under the CDSA, assisting another to retain benefits from any criminal activity and/or conduct is an offence.

3.2. **"Terrorist financing"** involves the raising and processing of funds that may come from legitimate or criminal sources to supply terrorists with resources to carry out their terrorist activities.

a) Under the TSOFA, a terrorist is defined as anyone who commits, or attempts to commit, any terrorist act, participates in, or facilitates the commission of any terrorist act, and includes any person set out in the First Schedule of the TSOFA.

b) Terrorists require funds to carry out acts of terrorism, and terrorism financing is the act of providing these funds.

c) Unlike money laundering, it is important to note that the sources of terrorism financing may be illegitimate but can also be financed from legitimate sources. In addition, terrorism financing does not always need to involve large sums of money; thus, it can be difficult to detect, and staff should remain vigilant.

4. MANAGEMENT OVERSIGHT

4.1. The Board of Directors (the "Board") has ultimate responsibility for overseeing AML/CTF measures at CFL. The Board appoints the Audit and Risk Committee (ARC) to assist in ensuring that the organisation's AML/CTF policies and procedures are effective and comply with relevant laws and regulations.

4.2. The ARC shall have full authority to implement and enforce this policy and its accompanying procedures (if any). All questions, comments and/or inquiries regarding this policy and its accompanying procedures (if any) should be directed to the ARC.

4.3. ARC shall appoint a CFL staff to function as the designated AML Compliance Officer ("**Officer**") to assist the ARC in implementing and carrying out AML / CTF measures, and promoting compliance with applicable AML / CTF laws and regulations.

4.4. A table below outlining the responsibilities of various roles is provided to ensure a clear division of duties. This structure ensures effective AML compliance oversight by the ARC and execution by the AML Compliance Officer.

Audience	Roles & Responsibilities
Board	Provides overall guidance on AML/CTF measures with support from the Audit and Risk Committee (ARC). Appoints and delegates AML/CTF oversight to the ARC.

Audit and Risk Committee ("ARC")	Oversees, approves policies, monitors effectiveness, and ensures adequate resources. **Key Responsibilities:** **Oversight and Governance:** a. **Review and Approve Policies:** Approve AML/CTF policies and procedures. b. **Monitor Compliance:** Ensure adherence to CDSA, TSOFA, and other relevant AML/CTF regulations in Singapore. c. **Assess Risk Management:** Evaluate AML risk assessment and management strategies. **Reporting and Communication:** d. **Report to the Board**: Update the Board on AML program status and significant issues. e. **Review Suspicious Activity Reports highlighted by AML Compliance Officer:** Ensure effective procedures for handling and escalating Suspicious Transaction Reports (STRs). **Training and Awareness:** f. **Oversee Training Programs:** Ensure AML training is effectively developed and implemented. **External Communication:** g. **Liaise with Regulators**: Provide direction to the AML Compliance Officer for communication, liaise with regulators, and review audit recommendations.
AML Compliance Officer ("Officer")	**Key Responsibilities:** h. **Implement AML Policies:** Develop and execute AML procedures as approved by the ARC. i. **Due Diligence and Risk Assessment:** Verify legitimacy of funds and transactions, and assess the AML risk profile. j. **Suspicious Activity Reporting:** Investigate suspicious activities, prepare, and submit STRs to the relevant authorities. k. **Compliance Monitoring:** Ensure adherence to AML policies, address non-compliance, and maintain records.

	l. **Training and Awareness:** Deliver AML training programs to all personnel. m. **Internal Reporting:** Report to the ARC on AML compliance, investigations, and suspicious activities.
Finance Support Services	**a. Monitor Funds Flow:** Determine if the transactions align with CFL's expectations and activities. Transactions requiring further scrutiny will be promptly reported to the Officer, including those flagged in Appendix B.
Employees and Volunteers	All staff and volunteers must adhere to the procedures set out in this policy and report any suspicious activities to the Officer.

5. SOURCES OF FUNDS AND DESTINATION OF FUNDS

All sources of funds must be legitimate, and due diligence must be conducted to verify their origin. CFL's main source of funding is the grant from Caritas Singapore, an IPC.

5.1. Sources and Modes of Donations

Apart from the grant from Caritas Singapore, CFL accepts donations from individuals, external corporations, and organisations through various methods, including cheques, PayNow, internet bank transfers, and the Giving.sg website.

5.2. Destination of Funds

Funds are used for the general operational needs for CFL, in accordance of approved programmes and actitivies to achieve the Vision and Mission of CFL.

CFL may explore collaboration opportunities and potentially extend funding to other recipients such as family ministries under the CFL umbrella, non-profit organisations, community groups, educational institutions, and governmental agencies, subject to Board approval.

6. DUE DILLIGENCE PROCESSES

CFL implements due diligence measures to ensure that its financial activities are conducted with integrity and in compliance with regulatory requirements. This section outlines the procedures for performing due diligence on the identity of persons or entities it has dealings with ("Third Party", e.g. donors, beneficiaries etc), and the source

of any funds paid to CFL. The objective is to help CFL determine the ML/TF risks and take appropriate measures to address them.

6.1. Donor Identification Framework

The measures to be performed by CFL to verify the identity of a Third Party are referred to generally as "Know Your Customer" ("**KYC**") procedures. KYC procedures generally comprise the following measures: (i) due diligence processes ("**DD**") and (ii) enhanced due diligence processes ("**EDD**").

6.1.1. DD generally refers to the collection of information from a Third Party to enable CFL to verify the identity of such Third Party and its beneficial owner (if any) and to assess the AML / CTF risk associated with such Third Party and its beneficial owner (if any).

6.1.2. EDD refers to the collection of additional information, consistent with and as required by the risks identified by CFL, in connection with a Third Party and its beneficial owner (if any).

6.2. Screening

6.2.1. As part of CFL's due diligence process on its donors and beneficiaries, it will carry out, as practicable as possible, reasonable checks (at least DD) on the identity of:

a) significant donors (defined as those donating S$10,000 & above);
b) new beneficiaries (i.e. a beneficiary who CFL has not dealt with or serviced in the preceding 24 months).

6.2.2. The level of due diligence, whether standard (DD) or enhanced (EDD), will be based on the specifics of each Third Party and their associated risk. Higher perceived risks require EDD and more detailed verification of the Third Party's identity.

6.2.3. The requirements of EDD are dependent on the below risk profile of the Third Party and/or its beneficial owner (if any). These include a person who is:

a) a politically exposed individual (PEP), or a family member or close associate of a PEP;
b) a resident of or originates from a country on the FATF list of high-risk countries (www.fatf-gafi.org/countries/#high-risk); or
c) is assessed to have higher ML/TF risks.

6.2.4. Refer to Appendix A for the detailed due diligence procedures.

6.2.5. Appendix B contains a non-exhaustive list of red flags that should be reported to ARC if observed. If a red flag is spotted, the ARC should be notified and will investigate the red flag and take action consistent with this policy and all applicable AML Laws.

6.2.6. CFL reserves the right to refuse any donation if there is reason to believe that accepting it would violate any AML regulations or if it originates from illegal activities.

6.3. Assessment and Reporting of Suspicious Transaction

6.3.1. Any individual who suspects or is aware of suspicious activities or discrepancies that may indicate money laundering, terrorism financing, or other illegal activities must file a Suspicious Transaction Report (STR) with the Suspicious Transaction Reporting Office (STRO). Failure to report may be considered a criminal offence under the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 (CDSA) and the Terrorism (Suppression of Financing) Act 2022 (TSOFA). SPF | STRO - Suspicious Transaction Reporting Office

6.3.2. An STR must be filed if:

a. There are reasons to suspect that any property is connected to criminal activity.
b. There is possession, custody, or control of any property or transaction information related to terrorism or terrorist entities.

6.3.3. The Officer must promptly report any Suspicious Transactions to the ARC and Board. If the Board determines that the concerns suggest illegal activity, they will instruct the Officer to file an STR.

6.3.4. An STR provides information about suspicious transactions and is used when there is a reason to believe that property is involved in criminal conduct. It is considered a provision of information rather than a crime complaint, and the STRO will decide on further actions.

6.3.5. An STR can be lodged by electronic filing on the STRO Online Notices and Reporting e-services platform (“SONAR”) via police.gov.sg/sonar.

7. RECORD KEEPING AND DOCUMENTATION

7.1. CFL shall maintain documents and records made or obtained through CFL's due diligence process (by way of original documents, photocopies of original documents or computerised or electronic form) for at least five (5) years after termination of CFL's relationship with the Third Party, or after the date of a transaction (for occasional donations and provision of services to beneficiaries).

8. RISK ASSESSMENT

8.1. CFL recognises that it may be exposed to the risk of money laundering and terrorist financing due to the nature of its operations. To manage and mitigate these risks, CFL will undertake annual risk assessments to identify potential vulnerabilities.

8.2. This policy should be read in conjunction with the Enterprise Risk Management Policy, which is designed to identify potential events and trends (which are commonly defined as 'Risks') that may significantly affect CFL's ability to achieve its strategic goals or maintain its operations, either positively or negatively.

9. ONGOING MONITORING OF PROGRAMMES AND FUND FLOWS

9.1. CFL is committed to ensuring that funds are used solely for their intended charitable purposes and not misused for illicit activities, including money laundering and terrorist financing.

9.2. To achieve this, ongoing monitoring of programmes and the usage of funds is essential. This includes:

a. Regular Reporting: All programmes and projects must submit financial and operational reports detailing how funds are allocated and spent;

b. Budget Reviews: Annual reviews of programme budgets to ensure spending is aligned with approved budgets and charitable objectives. Any discrepancies must be investigated and justified;

c. Disbursement Controls: All fund disbursements must go through a pre-approved process, ensuring that payments are made to legitimate vendors, contractors, or beneficiaries. Bank transfers will be the preferred method of payment over cash to reduce the risk of misuse.

9.3. CFL Finance Support Services shall regularly monitor the flow of funds in and out of CFL's accounts and consider whether the fund flows are consistent with CFL's expectations and activities, as well as whether the fund flows reflect activity consistent with the possibility of money laundering activity. Transactions requiring further scrutiny will be promptly reported to the Officer, including those flagged in Appendix B.

9.4. This policy should be read in conjunction with the Service Standards Policy and Section H - Grant Making Policy of the Finance Manual, which sets out the key principles for CFL in issuing grants.

10. TRAINING AND AWARENESS

10.1. CFL shall ensure that its employees attend ongoing training and raise awareness on the risks of ML/TF by educating them on the Anti-Money Laundering/Counter Financing of Terrorism (AML/CFT) requirements, including this policy.

10.2. Training will be conducted for:

a. New staff as part of the onboarding process and
b. On an annual basis for CFL staff.

10.3. CFL shall record the names of the employees who have undergone such training (together with the corresponding date(s) of such training) and keep such records for at least five (5) years.

11. REVIEW OF POLICY

11.1. This policy will be reviewed annually or as required due to changes in legislation, regulation, or the charity's activities.

12. REFERENCES

- Protecting Your Charity Against Money Laundering and Terrorist Financing, Office of the Commissioner of Charities, May 2015;
- Terrorist Financing Risk Mitigation Toolkit for Charities, Office of the Commisioner of Charities;
- Charities Lean Forward – Strengthen Your Charities Against Money Laundering and Terrorist Financing, Office of the Commissioner of Charities, November 2023;

- Countering Money Laundering and Terrorism Financing in Charities, Office of the Commissioner of Charities, November 2023.

Appendix A - Due Dilligence Process

Step 1:

CFL will confirm the significant donor's identity and sources of funds.

1. For Individual Donors, screening will be done via recorded phone call or email, for audit trail purposes. In view of respecting donor confidentiality, only the Officer may contact donors.

2. The Officer will call (recorded) or email the donor to obtain the following information:
   a. Full Name as appears in NRIC/Passport
   b. Occupation/Professional Status
   c. Residential address
   d. Email address
   e. Employer or name of business if self-employed
   f. Source of funds

3. If the donor is NOT a Singapore citizen or Permanent Resident of Singapore, additional questions (in addition to the above) should be asked to ascertain:
   a. Basis of stay in Singapore (Employment Pass or S Pass or any other legal basis, nexus to Singapore identification documents may be required for verification)
   b. How long the donor has been staying in Singapore.

4. For Corporate Donors (including Foundations and Trusts), screening will be done via ACRA checks to determine:
   a. If the company is local or foreign-owned (whether in high-risk jurisdictions)
   b. Nature of business
   c. The ultimate beneficiary owner/shareholder
   d. Place of incorporation
   e. Paid up capital of the company

5. EDD measures below must be performed for stakeholder(s) assessed to be of higher risk, for example, if the stakeholder is located in jurisdictions subject to call-for-action and is under increased monitoring by the FATF or in conflict zones. These measures include:

   a. Obtain additional information about the Third Party, including their business or personal background, financial history, and the purpose of transactions.
   b. Verify the identity and legitimacy of the Third Party through independent sources or documentation (e.g., financial statements, business licenses).
   c. Conduct ongoing monitoring of transactions and relationships to identify and address any changes in risk profile.

d. Review and document the rationale for applying EDD and any additional findings.

The above screening guidance is not meant to be exhaustive as the diligence process involves scrutiny and, depending on answers to specific questions, may warrant further checks and/or escalation to ARC. Discretion and judgment need to be carefully exercised and when in doubt and/or Red Flags (Refer to Appendix B) appear, staff are encouraged to escalate to the ARC for guidance.

Step 2:

Upon receiving the donor's information, designated staff will proceed to process their donation based on donor profiles to match against their giving.

Step 3:

The Officer will also perform some screening on any negative news on donors against the following information sources:

- Searches via the Internet and/or database subscription for adverse media reports or whether public concerns have been raised about the donors or their activities.

- Searches on government registers to ascertain whether past instances of regulatory action had been taken against an individual and/or entity. From time to time, government agencies or regulatory authorities (e.g., the Office of the COC, MAS, ACRA) may publish information on formal regulatory and enforcement actions for breaches of laws and regulations administered under their purviews.

    - Ministry of Home Affairs: IMC-TD website (https://www.mha.gov.sg/what-we-do/managing-security-threats/countering-the-financing-of-terrorism);

    - UN sanctions lists from the Monetary Authority of Singapore website (https://www.mas.gov.sg/regulation/anti-money-laundering/targeted-financial-sanctions/lists-of-designated-individuals-and-entities); and

    - Financial Action Task Force ("FATF") list of high-risk countries (https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)

If the search returned results with similar names (either exact match or partial match) to the searched name, staff should utilise other factors, such as identification document, date of birth, gender, citizenship, etc., to determine that the profiles are not the same person.

If a match of negative news is found, the AML Compliance Officer is to escalate to ARC for handling.

Step 4:

On an annual basis, the Internal Auditor appointed by ARC will perform a random check on this process to ensure adherence.

Step 5:

Ensure all documents regarding donor information and the screening process are kept for 5 years for record purposes.

Step 6:

The Officer will, as soon as practicable, advise ARC and the Board if any donor irregularity or suspicious activity is discovered and will adopt the following actions:

a. No tipping of suspicious reporting to the donor or any party
b. If the Board determines that the concerns suggest illegal activity, they will instruct the Officer to file an STR
c. Notify Finance Support Services to ringfence suspicious funds (which have yet to be expended or disbursed) pending instructions from the STRO and a decision from the Board on what to do with the funds.

Appendix B - Red Flags/Suspicious Indicators of ML/TF

Charities should also look out for red flag indicators that may be a warning sign of unusual activities, which could include:

Incoming Funds:

- Donation amounts that appear to be more than the usual amount that particular profile(s) of donor(s) would typically make;
- Donations made through third parties instead of the donors themselves without apparent legitimate purposes;
- Unusual request for refund of donations;
- Donor splits his/her/their donation in more than a single sum. This tactic is used mostly to avert attention to an otherwise large lump sum;
- Unusual requests from donors to redirect part of the donations to unknown third parties for purposes that may be incongruent with the charity's charitable objects;
- Donations involving virtual assets, especially where the ownership of the virtual assets cannot be easily traced to the donor(s);
- Donor carries a passport from a high-risk jurisdiction such as Iraq, Iran, Sudan, St Kitts and Nevis, Grenada, Malta, Antigua and Barbuda, Saint Lucia, Dominica, Cyprus, Vanuatu, Montenegro, Latvia, or countries where the rule of law is not always clear, e.g. Cambodia, Laos, African sub-continent countries. The list is not exhaustive but is meant to show examples of countries where movements of monies are less/not regulated, hence open and more susceptible to money laundering or terrorist financing activities;
- Similarly, this applies to corporate donors if the company's place of incorporation is in these countries;
- The corporate donor is a shell company, i.e. a company with minimum paid-up capital, such as a $2 company or foreign incorporated company with no real business other than a thinly capitalised holding company.

Outgoing Funds

- Request for remittance of donations/funds to multiple foreign bank accounts even though the beneficiary is a single entity;

- Request by a beneficiary not to remit donations/funds through banking facilities but to pass it to them in cash;

- Request to structure transactions such that transaction reporting can be avoided (e.g. by requesting that numerous transactions for smaller amounts be made to the same beneficiary);

- Insufficient/vague/suspicious documentation, descriptions and details for instructions for payments;

- Use of cash couriers to transfer the charity's funds to areas with known terrorist activity;

- Request to remit donations/funds to, transfer resources to and/or carry out activities in countries/areas that are:

    - identified as subject to targeted financial sanctions by, e.g. UN Security Council resolutions;
    - subject to call-for-action and/or under increased monitoring by the FATF;
    - where terrorist entities have a substantial presence.