Anti-Money Laundering and Countering Terrorism Financing Policy

GiveSG Pte. Ltd.

UEN: 202556963R
Registered Address: 7 Temasek Boulevard, #12-07, Suntec Tower One, Singapore 038987
Platform: give.com.sg
Approved By: Managing Director

---

1. Context

Money laundering refers to the process where criminals attempt to disguise the proceeds of crime as legitimate funds. Terrorism financing refers to the raising, movement, or use of funds, whether from lawful or unlawful sources, to support terrorist activities.

As an online charitable crowdfunding platform, GiveSG Pte. Ltd. ("GiveSG") recognises that fundraising platforms may be exposed to risks where donors, campaign creators, fundraisers, or other parties attempt to misuse charitable giving channels for improper purposes.

GiveSG's role is to provide a safe, transparent, and accountable online platform for registered charities and Institutions of a Public Character ("IPCs") in Singapore to raise funds for legitimate charitable purposes. GiveSG currently operates only in Singapore and does not support the outflow of funds outside Singapore.

GiveSG notes that the Commissioner of Charities' Code of Practice for Online Charitable Fund-Raising Appeals is intended to promote legitimacy, accountability, and transparency in charitable appeals hosted on crowdfunding platforms in Singapore. GiveSG has submitted its application to subscribe to the Code and is awaiting approval. (Ministry of Culture, Community & Youth)

---

2. Policy Statement

GiveSG is committed to preventing its platform, services, payment flows, campaign pages, and charitable fundraising activities from being misused for money laundering, terrorism financing, fraud, sanctions evasion, or other unlawful activities.

GiveSG will take reasonable and proportionate steps to:

a. verify charities and IPCs before allowing them to raise funds on the platform;
b. review campaigns before they go live;
c. monitor donations, refunds, and unusual transaction patterns;
d. escalate suspicious transactions or activities internally;
e. pause campaigns or freeze payouts where appropriate;
f. cooperate with charity partners, payment processors, regulators, and law enforcement agencies where necessary; and
g. lodge a Suspicious Transaction Report ("STR") where GiveSG determines that there are reasonable grounds for suspicion.

---

3. Policy Goals

The goals of this policy are to:

a. reduce the risk of GiveSG being used as a conduit for money laundering or terrorism financing;
b. ensure that only registered charities and legitimate causes in Singapore are onboarded onto the platform;
c. establish clear procedures for charity due diligence, campaign verification, transaction monitoring, refund reviews, and payout controls;
d. ensure that staff and relevant personnel understand how to identify suspicious activities;
e. provide a clear escalation process for suspected money laundering or terrorism financing concerns; and
f. maintain proper records to support accountability, auditability, and regulatory cooperation.

---

4. Scope

This policy applies to:

a. GiveSG Pte. Ltd.;
b. all directors, employees, advisors, contractors, and authorised representatives of GiveSG;
c. all charities and IPCs onboarded onto the GiveSG platform;
d. all crowdfunding campaigns hosted on give.com.sg;
e. all donors and donations processed through the platform;

f. all refunds, chargebacks, and donation disputes; and
g. all payouts or fund disbursements to charity partners.

---

5. Governance and Responsibility

Overall responsibility for this policy rests with the Managing Director of GiveSG.

Managing Director:
Dorian Manrique
Email: Dorian@give.com.sg

The Managing Director is responsible for:

a. approving this policy;
b. overseeing AML/CTF controls and escalation decisions;
c. deciding whether a Suspicious Transaction Report should be lodged;
d. approving the pausing of campaigns or freezing of payouts where necessary; and
e. ensuring the policy is reviewed periodically.

The Senior Advisor, Compliance & Risk may advise the Managing Director on suspicious activity reviews, risk controls, internal procedures, and appropriate follow-up actions.

---

6. Platform Operating Principles

GiveSG shall operate according to the following principles:

a. GiveSG will only onboard registered charities and legitimate causes in Singapore.
b. GiveSG will not support fundraising for unverified private individuals, overseas entities, or unregistered organisations.
c. GiveSG will not permit the outflow of funds outside Singapore.
d. Donations will be processed through Stripe.
e. Donor funds will be disbursed to the relevant charity on a monthly basis.
f. Funds will be settled within seven working days after the end of each month, subject to review, verification, payment processor timelines, and any ongoing investigations.
g. Refunds will be handled by GiveSG.
h. GiveSG reserves the right to pause campaigns, delay payouts, request supporting documents, reject transactions, or escalate suspicious matters where necessary.

---

7. Charity Onboarding Due Diligence

Before a charity or IPC is approved to raise funds on GiveSG, the platform shall conduct due diligence checks.

7.1 Documents Required

GiveSG shall request the following documents from each charity:

a. Certificate of Incorporation;
b. proof of charitable status and registration with regulatory authorities;
c. most recent bank statement; and
d. latest financial statement or annual report.

Additional documents may be requested where GiveSG considers it necessary.

7.2 Verification Checks

GiveSG shall verify the charity's status against the Charity Portal before approving the charity's account.

The verification process may include:

a. confirming the charity's registered name;
b. confirming its UEN or registration number;
c. checking whether it is a registered charity or IPC;
d. confirming that the bank account belongs to the charity;
e. confirming the authorised representative;
f. reviewing the charity's latest annual report or financial statement; and
g. checking whether the proposed fundraising activities are consistent with the charity's stated charitable objects.

7.3 Approval

Only charities that pass GiveSG's onboarding checks may be approved to use the platform.

GiveSG reserves the right to reject, suspend, or terminate a charity's access to the platform where:

a. the charity fails to provide required documents;
b. the information provided is incomplete, inaccurate, or inconsistent;
c. the charity's registration status cannot be verified;
d. the charity's campaign purpose appears unclear, misleading, or inconsistent with its charitable objects; or
e. GiveSG identifies potential money laundering, terrorism financing, fraud, reputational, or regulatory concerns.

8. Campaign Verification

Approved charities may upload their own campaigns onto the platform. However, campaigns must be reviewed and verified by GiveSG before going live.

GiveSG's campaign review may include:

a. checking that the campaign is created by an approved charity;
b. confirming the campaign purpose;
c. checking that the beneficiary, cause, or programme is clearly described;
d. ensuring that the use of funds is reasonably clear;
e. reviewing the campaign wording for misleading or exaggerated claims;
f. checking whether supporting documents or charity confirmation are required; and
g. ensuring the campaign does not appear to raise funds for unlawful, political, extremist, foreign, private, or non-charitable purposes.

GiveSG may reject, amend, pause, or remove any campaign that does not meet its internal standards.

---

9. Donor Information and Tax Deduction Data

Donors may choose to donate anonymously on the public-facing campaign page.

GiveSG may collect the following donor information:

a. donor name;
b. email address;
c. donation amount;
d. payment details processed through Stripe; and
e. identification number where required for tax deduction purposes.

Donors may choose not to provide their identification number if they do not wish to claim tax deduction.

GiveSG collects identification information only where required to support the charity's tax deduction filing obligations. Such information shall be handled with care and used only for the relevant donation, reporting, tax deduction, compliance, and record-keeping purposes.

---

10. Transaction Monitoring

GiveSG shall monitor donations and platform activity for unusual or suspicious patterns.

Transaction monitoring may include manual checks and payment processor alerts.

The following transactions shall trigger manual review:

a. any single donation above S$10,000;
b. repeated small donations from the same donor, card, email address, IP address, or related identifiers;
c. multiple failed payment attempts followed by successful payments;
d. donations followed by urgent or unusual refund requests;
e. donations made using inconsistent donor details;
f. donations that appear inconsistent with the donor's known profile or declared intention;
g. donations suspected to be linked to fraud, stolen cards, compromised payment methods, or chargeback abuse;
h. donations connected to high-risk jurisdictions, sanctioned persons, or suspicious networks; and
i. any transaction that appears unusual based on GiveSG's experience and judgement.

---

11. Suspicious Activity Red Flags

The following situations may be considered suspicious. This list is not exhaustive.

11.1 Donor and Donation Red Flags

a. A donor makes a large donation and soon after requests a refund without a reasonable explanation.
b. A donor requests that funds be redirected to a private individual, unrelated third party, or different organisation.
c. A donor insists on anonymity while making an unusually large donation.
d. A donor provides incomplete, false, inconsistent, or suspicious contact details.
e. A donor uses multiple cards, names, emails, or payment attempts for the same or similar donation purpose.
f. Multiple donations are made in smaller amounts in a way that appears designed to avoid review.
g. A donor appears to be acting on behalf of an undisclosed third party.
h. A donation is linked to a country, person, organisation, or activity associated with heightened ML/TF risk.
i. The donor becomes defensive, evasive, or unwilling to provide clarification when asked reasonable questions.

11.2 Charity and Campaign Red Flags

a. A charity refuses or delays providing onboarding documents.
b. A charity's bank account details do not match the charity's official name.
c. A campaign purpose is unclear, vague, misleading, or inconsistent with the charity's

registered charitable objects.
d. A campaign appears to raise funds for a private person or private benefit without clear charity oversight.
e. The campaign creator requests urgent payout before normal settlement timelines.
f. The charity requests funds to be paid into an account not belonging to the charity.
g. Campaign descriptions contain inconsistent beneficiary information.
h. The campaign appears to involve foreign causes, overseas transfers, political activity, extremist content, or non-charitable purposes.
i. There are complaints from donors, the public, regulators, or charity representatives regarding the campaign.

11.3 Refund and Chargeback Red Flags

a. A donor requests a refund to a different card, account, or person.
b. A donor requests a refund shortly after making a large donation.
c. A donor repeatedly donates and requests refunds.
d. Refund requests are inconsistent with Stripe's transaction records.
e. Refund requests are accompanied by pressure, urgency, threats, or refusal to provide reasonable information.
f. Refund activity suggests possible use of the platform to test stolen cards or move funds.

11.4 Platform Misuse Red Flags

a. Unauthorised use of GiveSG's name, logo, campaign links, or branding.
b. Third parties claiming to represent GiveSG without authorisation.
c. Attempts to create fake charity campaigns.
d. Attempts to impersonate registered charities or their staff.
e. Attempts to use GiveSG to solicit donations outside the platform without authorisation.
f. Suspicious traffic, automated activity, or abuse of donation forms.

---

12. Manual Review Procedure

Where a transaction, donor, charity, campaign, refund, or payout is flagged for review, GiveSG shall take appropriate steps based on the nature and seriousness of the concern.

The review may include:

a. checking the donation record and Stripe transaction details;
b. reviewing the donor's name, email, donation amount, and transaction pattern;
c. contacting the donor for clarification where appropriate;
d. contacting the charity for confirmation or supporting documents;
e. reviewing the campaign purpose and supporting materials;
f. checking whether similar suspicious activity has occurred;
g. consulting the Senior Advisor, Compliance & Risk;

h. escalating the matter to the Managing Director; and
i. deciding whether to approve, reject, refund, pause, freeze, or report the matter.

All material findings should be documented.

---

13. Refund Controls

Refunds will be handled by GiveSG.

Before processing a refund, GiveSG may review:

a. the donor's identity and contact information;
b. the donation amount;
c. the reason for the refund request;
d. whether the refund request is consistent with normal donor behaviour;
e. whether the refund should be made only back to the original payment method;
f. whether the charity has already received or used the funds; and
g. whether there are any suspicious circumstances.

Where a refund request appears suspicious, GiveSG may delay the refund pending review.

GiveSG should generally avoid refunding donations to a different person, account, card, or payment method from the original source unless there is a clear, documented, and approved reason.

---

14. Payout Controls

Donor funds will be disbursed to charities monthly, within seven working days after the end of each month, subject to review and any pending issues.

GiveSG or the charity may pause a campaign or freeze payouts pending review where there are concerns relating to:

a. suspected money laundering;
b. suspected terrorism financing;
c. suspected fraud;
d. suspected misuse of funds;
e. unclear campaign purpose;
f. donor complaints;
g. regulatory enquiries;
h. payment processor alerts;

i. chargeback or refund abuse; or
j. reputational or legal risk.

Where payouts are paused or frozen, GiveSG shall document the reason and follow up with the relevant charity, donor, payment processor, or authority as appropriate.

---

15. Escalation Procedure

All suspected ML/TF concerns must be escalated to the Managing Director.

Escalation Contact:
Dorian Manrique
Managing Director
Dorian@give.com.sg

The Managing Director may consult the Senior Advisor, Compliance & Risk before deciding the next course of action.

Possible actions include:

a. no further action, with the reason documented;
b. request for further information from the donor or charity;
c. enhanced monitoring of the donor, charity, or campaign;
d. rejection of the donation;
e. refund to the original payment method;
f. pausing or removing the campaign;
g. freezing or delaying payout;
h. suspending or terminating the charity's platform access;
i. notifying the charity;
j. notifying Stripe or other relevant service providers;
k. reporting the concern to the Commissioner of Charities where appropriate; and/or
l. lodging a Suspicious Transaction Report.

Concerns about a charity or fund-raiser may also be reported to the Charities Unit where appropriate. The Charity Portal states that concerns about a charity or fund-raiser may be reported to MCCY Charities Unit. (Charity Portal)

---

16. Suspicious Transaction Report

Where GiveSG determines that there are reasonable grounds to suspect money laundering, terrorism financing, or other serious offences, the Managing Director shall decide whether to lodge a Suspicious Transaction Report.

Where required, an STR may also be submitted to:

Head, Suspicious Transaction Reporting Office
Commercial Affairs Department
391 New Bridge Road #06-701
Police Cantonment Complex Block D
Singapore 088762 (Singapore Police Force)

The STR should include, where available:

a. details of the suspicious transaction or activity;
b. donor information;
c. charity or campaign information;
d. donation amount and date;
e. payment transaction records;
f. refund or chargeback details;
g. supporting documents;
h. communications with the donor or charity; and
i. GiveSG's internal review notes.

GiveSG shall not inform the donor, campaign owner, or any unauthorised party that an STR has been or may be lodged, where doing so may compromise any investigation.

---

17. Use of GiveSG's Name, Logo, and Platform

The use of GiveSG's name, logo, platform, campaign links, or branding for fundraising purposes must be authorised.

If GiveSG becomes aware that any person or organisation is using GiveSG's name, logo, campaign pages, or branding without authorisation, the matter shall be escalated to the Managing Director.

GiveSG may take appropriate action, including:

a. requesting immediate removal of unauthorised materials;
b. notifying the affected charity;
c. issuing a clarification to donors or the public;
d. suspending the relevant campaign or account;
e. reporting the matter to the relevant authority; and/or
f. taking legal action where necessary.

---

18. Record Keeping

GiveSG shall retain relevant AML/CTF records for at least five years.

Records may include:

a. charity onboarding documents;
b. verification checks;
c. campaign approval records;
d. donor transaction records;
e. tax deduction information provided by donors;
f. refund and chargeback records;
g. payout records;
h. suspicious activity review notes;
i. escalation records;
j. STR filing records, where applicable; and
k. training and policy review records.

Records shall be kept securely and accessed only by authorised persons.

---

19. Training and Awareness

GiveSG shall provide periodic AML/CTF awareness briefings to relevant staff, advisors, contractors, and authorised personnel.

Training may include:

a. basic understanding of money laundering and terrorism financing risks;
b. charity onboarding red flags;
c. campaign verification procedures;
d. donor and donation red flags;
e. refund and chargeback risks;
f. transaction monitoring procedures;
g. escalation procedures;
h. STR filing awareness; and
i. data handling and confidentiality requirements.

New staff involved in onboarding, operations, payment review, campaign approval, donor support, or charity support should receive AML/CTF briefing as part of onboarding.

---

20. Policy Review

This policy shall be reviewed periodically by the Managing Director, with input from the Senior Advisor, Compliance & Risk where appropriate.

The policy may be reviewed earlier if there are:

a. changes to GiveSG's business model;
b. changes to payment processing arrangements;
c. changes to regulatory expectations;
d. significant suspicious activity incidents;
e. feedback from charity partners, Stripe, regulators, or law enforcement agencies; or
f. expansion beyond the current Singapore-only operating model.

Review Log

Version	Date of Review	Approved By
1.0	15th February 2026	Managing Director