

Malaria Consortium

Anti-Money Laundering and Terrorist Financing Policy



Last updated: October 2018
Author: Finance Director
Review date: October 2020

1. Purpose and context

This policy aims to prevent opportunities for money laundering activities to occur within the organisation.

This policy applies to all persons working for us or on our behalf in the UK in any capacity whether paid or unpaid (the “**staff**”) and wherever located, unless local legal requirements are more rigorous or the application of this policy under local law would be illegal.

2. Principles and Scope

The organisation is committed to actively preventing and taking measures to guard against being used as a channel for money laundering activities and terrorism financing activities and any other activity that facilitates money laundering or the funding of terrorist or criminal activities.

The organisation has a duty to protect the public funds it receives and its resources must not be used to support criminal or terrorist purposes. The purpose of this anti-money laundering and terrorist financing policy is, therefore, to put in place the systems, procedures and controls necessary to ensure that it can manage the risk of becoming involved in financing or otherwise supporting money laundering or terrorist activity.

This policy will:

1. Set out the responsibilities of staff in observing and upholding our zero-tolerance approach to money laundering and terrorist financing; and
2. Provide information and guidance to on how to recognise, deal with and counter money laundering and terrorist financing.

When working with the organisation all staff will receive training on this anti-money laundering and terrorist financing policy as part of their induction.

All staff have an obligation to familiarise themselves with the organisation’s procedures on identification and prevention of money laundering and terrorist financing activity set out herein and are required to conduct their work in a manner such that the opportunity and incidence of money laundering and terrorist financing activity is prevented or mitigated to the greatest possible extent.

All staff should actively seek to:

- prevent money laundering and terrorist financing activity occurring;
- identify potential incidences of money laundering and terrorist financing activity; and
- report suspected money laundering and terrorist financing activity,

In each case, in accordance with the terms of this policy.

3. What is “Money Laundering”?

Money laundering is essentially the process by which criminals attempt to conceal the true origin or ownership of proceeds of their criminal activities, such that they appear to come from a legitimate source.

The substantive law regarding money laundering is set out in the Proceeds of Crime Act 2002 (the “POCA”). The offences under the POCA criminalise both the process of laundering money and the failure to report suspicions of money laundering.

The principal money laundering offences under the POCA are:

- a) concealing, disguising, converting or transferring criminal property (being any benefit or property representing the same from criminal conduct, including goods and money) out of the jurisdiction of England and Wales;
- b) entering into arrangements to facilitate money laundering; and
- c) acquisition, use and possession of criminal property.

All three of these offences require either a knowledge or suspicion of money laundering.

The POCA also contains a number of offences for those operating in the regulated sector relating to a person’s action or inaction upon discovering potential money laundering (i.e. failing to report or disclose and “tipping-off” someone who is being (or is about to be) investigated for money laundering). Although the organisation does not currently operate in the regulated sector, in order to avoid being manipulated by money launderers or becoming associated with money laundering in general, this policy requires staff to report any knowledge or suspicion of money laundering (please see below).

It will, however, be an offence under the POCA for any person to prejudice a money laundering investigation. A person will commit this offence if they know or suspect that a money laundering investigation has, or is about to be, commenced in respect of another and makes a material disclosure to any other person which is likely to prejudice the investigation or interferes with any relevant material.

4. What is “Terrorist Financing Activity”?

Terrorism financing is essentially the provision of financial support, in any form, for terrorist activity or to those who encourage, plan or engage in terrorist activity.

The Terrorism Act 2000, as amended, establishes several offences in relation to engaging in or facilitating terrorism, as well as raising or possessing funds for terrorist purposes.

Money laundering and terrorist financing activity often display similar transactional features (e.g. concealment and disguise). However, money laundering focuses on the concealment or the criminal origin of funds whereas terrorist financing focuses on disguising the use of the relevant funds. The most significant difference, therefore, is that funds used for terrorist financing could originate from a legal source.

5. Application

The abuse of charities, such as the organisation, for money laundering or the financing of terrorist activities may take various forms including, without limitation:

- loans from donors as a means of laundering money (i.e. criminal proceeds would be paid to the organisation as a loan, used by the organisation and “laundered” when repaid to the donor);
- donations made with specific restrictions or instructions as to which partner or project is to be funded as a means of transferring funds overseas and disguising the origin (or potentially funding terrorist activity); and
- anonymous cash donations or donations through suspect third parties as a means of disposing of the proceeds of crime.

Suspicious activity can be more difficult to detect in jurisdictions where money laundering regulations are not as rigorous and funds may be transferred through unregulated channels.

The best defence against money laundering and the financing of terrorist activities remains good governance and vigilance.

Staff must undertake proper due diligence and ‘know your donor’ checks through the process, in relation to those individuals and organisations that give money to, receive money from or work closely with the organisation to safeguard against money-laundering and terrorist funding offences, to identify and take into account factors such as:

- the size of the donation;
- the source of funds; and
- the donor’s location,

and in each case, further verification checks when the donor is considered high risk.

Identifying suspected money laundering and terrorist financing is very much a matter of personal judgement. However, staff should consider for each transaction:

- Is there anything unusual about the manner in which the partner or supplier wishes to provide his goods?
- Is there anything unusual about the partner or suppliers’ conduct or behaviour?

The key, therefore, to identifying suspect transactions is to look out for exceptional features such as:

- receipt of an unusually large or unexpected donation in a single cash sum or series of cash sums;
- an inability to verify the identity of the donor;
- a request to act as a conduit for the passing of a donation to a second body which may or may not be another charity and any other and any other financial transfers to different accounts for an individual or organisation;
- cheques from several different accounts;
- unusual behaviour in connection with, or conditions on, when the money will become available and/or what it can be used for;

- complex banking and transfer arrangements;
- retention of a donation for a certain period of time with the attraction of retaining interest earned in the account, with the principal sum to be returned at the end of a specified, short, period (i.e. donations which are, in reality, some form of loan);
- named supplier is not the same as on the invoice as for payment
- payment involves unusual foreign currency transactions.
- secrecy about personal details required for the contract;
- providing a false address;
- where donations are conditional on particular individuals or organisations being used to do work for the charity where there is concern about those individuals or organisations; and
- where a charity is asked to provide services or benefits on favourable terms to the donor or a person nominated by the donor.

Note that this list is intended to be indicative rather than exhaustive. Being vigilant and looking for unusual payment methods or unusual conduct, as well as knowing the party in any transaction is paramount. Cash sums should be avoided and funds should be transferred to recognised banks only. Where funds are routed through other banks for payment, the route should be checked with the bank, for example on the transfer of staff salary payments.

6. Your responsibilities: reporting knowledge or suspicion of money laundering

You must ensure that you read, understand and comply with this policy.

The prevention, detection and reporting of money laundering and terrorist financing are the responsibility of all those working for Malaria Consortium or under its control. You are required to avoid any activity that might lead to, or suggest, a breach of this policy.

If any individual becomes aware or suspicious of any transaction it should be reported in accordance with Malaria Consortium's Whistleblowing Policy. Following the outcome of the investigation if deemed necessary by the Finance, Audit and Risk Committee the Finance Director will inform the National Crime Agency and may also report to the Charity Commission under its reporting serious incidents regime.

US Regulations

Under US regulations, when in the USA any staff member who accepts an amount of at least USD 10,000 in cash in one or more related transactions must complete and file IRS Form 8300 within 15 days of the date the cash was received. (Cash includes money orders, bank drafts and traveller's cheques). Therefore, staff should not accept any amount in cash in the USA of USD 9,999 or more.

7. Monitoring and Review

The implementation of the financial controls as per Malaria Consortium's Finance Manual is essential by all who work with and in the organisation. Training is to be provided to staff to ensure that they are familiar with the financial controls and know what actions to take if they suspect criminal financial abuse. Relevant internal control systems and procedures will be subject to audit under the internal audit process.

Malaria Consortium

The Green House, 244-254 Cambridge Heath Road,
London E2 9DA, United Kingdom

www.malariaconsortium.org

info@malariaconsortium.org

UK Registered Charity No: 1099776

malaria consortium
disease control, better health