

Practical Action

PROTECTING PRACTICAL ACTION FROM TERRORIST FINANCING POLICY

Version 0003.00

Date 1 March 2024

Scope All employees, Trustees,
Consultants and others
acting on behalf of Practical
Action or its subsidiaries.

**Review
Date** 1 March 2026

Approval required from	Finance Audit and Risk Committee (FAR)
Policy Owner:	Chief Financial Officer
Responsible Director:	Chief Operating Officer
Approval Date	February 2024

Queries:	Contact the Policy Owner
Exceptions:	Contact the Responsible Director

Table of Contents

1. Roles and responsibilities	3
Linked Practical Action policies	3
Further reading and resources	3
2. Policy Statement	4
3. Detail	4
4. Risks	4
Use of Practical Action’s name or reputation	4
Use of Charity Assets	4
Funders	5
Partners, Suppliers and Associates	5
Employees, Consultants, Directors or Trustees	5
5. Who should be Screened	5
Trustees, Directors, Staff and Volunteers	5
Consultants	5
Donors	5
Sub-grantees and Partners	6
Suppliers	6
Pre-qualified suppliers	6
6. The Screening Process	6
7. The Outcome	7
8. Confidentiality	7
9. Appendix	8
Appendix 1: The Internal Process	8
Appendix 2: USAID Partner Vetting	9


1. Roles and responsibilities:

- Clarifications on the policy content should be sought from the **policy owner**. Any changes required to the policy will be submitted through this the **policy owner** to the **responsible director**, for consideration.
- The **policy owner** is responsible for review of the policy every two years.
- Derogations from this policy require the **advance written approval** of the **responsible director**.
- The **responsible director** will seek formal approval of significant changes to this policy from the **Practical Action Board of Trustees** or their delegated representatives.

Linked Practical Action policies:

- Global Complaints (Whistleblowing) Policy - provides guidance on raising a concern or complaint. [Global-Complaints-and-Whistleblowing-Policy.pdf \(practicalaction.org\)](#)
- Protecting Practical Action from Financial Crime Policy - primary reporting of suspected fraud, bribery, money laundering or other financial abuse including investigations developing a *response* plan for reported suspicions [Financial-Crime-Policy-0002.00.a.pdf \(practicalaction.org\)](#)
- Conflict of Interest Policy - Gifts and Hospitality – defines what is acceptable in the acceptance and giving of gifts and hospitality
- Global Pre-Employment Screening Policy - outlines the required pre-employment screening checks
- Global Procurement Policy & Procurement Procedures

Further reading and resources:

- Charity Commission Guidance: Protecting Your Charity From Harm – *How to safeguard your charity from terrorism, fraud and other abuse*. [Protecting charities from harm: compliance toolkit - GOV.UK \(www.gov.uk\)](#)
-  USAID policy directives and required procedures for partner vetting [ADS Chapter 319 - Partner Vetting \(usaid.gov\)](#)
- Terrorism Act 2000, UK Public General Acts [Terrorism Act 2000 \(legislation.gov.uk\)](#) update Feb 2024.

2. Policy Statement

This policy applies to all Practical Action staff, trustees, consultants, partners, sub-grantees, donors and suppliers globally to ensure Practical Action supports the prevention of terrorist financing and/or avoids inadvertently supporting terrorist activitiesⁱ.

3. Detail

Practical Action, its staff and associates, seek to ensure that its activities and funds are never used to support terrorism or terrorist activities. We seek to comply with the letter, intent and spirit of anti-terrorism lawsⁱⁱ and in particular UK counter-terrorism legislationⁱⁱⁱ which specifies:

- Charity trustees, employees and volunteers are now under a **positive legal duty** to report their suspicions of terrorist financing offences^{iv} to the UK police. If they don't, they may be committing a **criminal offence**.
- Where the risks are high, we must screen stakeholders (trustees, directors, staff, consultants, volunteers, donors, sub-grantees, partners and suppliers) using a **screening process** (see *Section 6*) which compares individuals, entities and organisations against the list of **proscribed organisations** and **designated individuals** and **entities**. Whatever the level of risk, it is good practice to screen.
- A **designated person** (individual subject to financial restrictions in the UK) cannot be appointed as a trustee or Director of any Board within the charity.

4. Risks

Use of Practical Action's Name or Reputation

Funds may be raised in the name of a charity or charitable purposes, which are then used by the individuals (fundraisers) for supporting terrorist purposes, with or without the knowledge of the charity. Individuals supporting terrorist activity may claim to work for a charity and trade on its good name and legitimacy in order to gain access to a region or community that is difficult to reach. Sometimes the charity may simply provide the opportunity for terrorists to meet in order for them to stay under the radar. These activities may well take place undetected, without the knowledge of the charity or trustees.

Use of Charity Assets

Charity vehicles, property or funds could be used for terrorist activities.

Support for terrorism may be perpetrated or driven by funders, partners, suppliers, associates, employees, consultants, directors or trustees.

Funders

Funders who exercise some control over how funds are used, i.e. providers of restricted funds, may use the charity as a conduit to support terrorist activities, directly or indirectly.

Partners, Suppliers and Associates

A charity may give financial or other support to an organisation or partner that provides legitimate services, aid or relief. However, that organisation or partner may also support or carry out terrorist activities. In extreme cases, terrorists may try to set up an organisation, promoted as charitable but whose sole purpose is really to raise funds or use its facilities or name to promote or coordinate inappropriate and unlawful activities.

Employees, Consultants, Directors or Trustees

Those within a charity may also abuse their position for terrorist purposes. Effective due diligence and screening provides the best control against being party to terrorist activities.

5. Who should be screened?

The guidance below provides details of the **minimum standards** required by Practical Action and the roles with responsibility for carrying out the screening process.

For all internal stakeholders (trustees, directors, staff and volunteers), **your review and acceptance of this policy confers the right for Practical Action to carry out screening against your personal data.**

There may be instances where a particular donor has more stringent requirements for their projects (ie; USAID) and in such cases the donor requirements must be followed also.

Trustees, Directors, Staff and Volunteers

The Company Secretary is responsible for overseeing the necessary screening of all Trustees as part of the recruitment process.

The People & Culture contact is responsible for providing the necessary data for the screening to be conducted. This will include details for new staff and volunteers, as well as leavers so that they are taken off the data base.

All roles advertised for Practical Action state that successful candidates will be subject to pre-employment screening that includes financing terrorism.

Consultants

Finance Managers are responsible for providing data necessary for the screening of consultants for their country/region as part of the procurement process. The requirement for such screening should be clearly indicated in the consultant's subgrant/ subcontract.

Donors

The lead fundraising / business development manager is responsible for providing the data for screening against relevant donors, organisations and individuals wherever the donor is exercising

any control over how funds will be used. This is agreed upon completion of the Practical Action Public and Private Engagement Policy Assessment with the Donor and ideally before the receipt of funds. [Public-and-Private-Engagements-Policy-FINAL-2.pdf \(practicalaction.org\)](#)

Sub-grantees and Partners

Finance managers are responsible for carrying out screening against sub-grantees and partners. Screening will be undertaken at organisational level and also for key office holders including Directors/ Board members and Senior staff, in addition to project key personnel. This requirement must be clearly identified in the sub-grants or sub-contracts.

Suppliers

All suppliers with which the organisation directly engages will be subject to screening.

Pre-qualified suppliers should be screened as part of the assessment process. Finance Managers are responsible for providing data on shortlisted suppliers for all contracts over £1,000 (*in line with the Procurement Policy*) should be subject to screening, and this requirement should be made clear in any bid pack in the Terms of Reference. The person in charge of the procurement process is responsible for carrying out the necessary screening.

6. The Screening Process

Practical Action has appointed a data screening Security Company who provide a centralised database containing the following counter terrorism lists:

- United Nations Security Council Sanctions (entities & individuals)
- European Sanction EU (entities & individuals)
- HM Treasury (entities & individuals)
- OFAC Consolidated (OFCNS entities & individuals)
- OFAC Specially Designated Nationals (entities & individuals)
- World Bank Debarred Firms (entities & individuals)

In addition to the above for all USAID primary and secondary donor funded awards the excel file *SAM Exclusions Public Extract* [SAM.gov | Data Services](#) should also be reviewed and any questions about partner vetting directed to [Central Vetting Group](#) at cvg@usaid.gov. (*Appendix 2: USAID Partner Vetting.*)

If you become aware of a specific donor requirement that is not covered above, please contact the Chief Financial Officer

The Finscan operatives within Practical Action are tasked with entering stakeholder data into the centralised database. A primary screening is then undertaken with immediate results of any confirmed or potential matches. If a potential match is identified then this will be escalated to the relevant director or Chief Financial Officer, and at their discretion may suspended the relationship pending further enquiries. (*Appendix 1 : The Internal Process*).

Stakeholder records continue to be monitored as and when the terrorist lists are updated. The database will be reviewed regularly to ensure details are held only for those who have a

current/ongoing relationship with Practical Action. An audit trail is maintained in the system to provide evidence to donors and other interested parties of compliance with monitoring requirements.

7. The Outcome

If the outcome of any due diligence or screening, results in any individual or organisation being linked to any form of terrorist activities, the relevant Director will confirm the decision on terminating the relationship, contract of employment or subaward/subcontract.

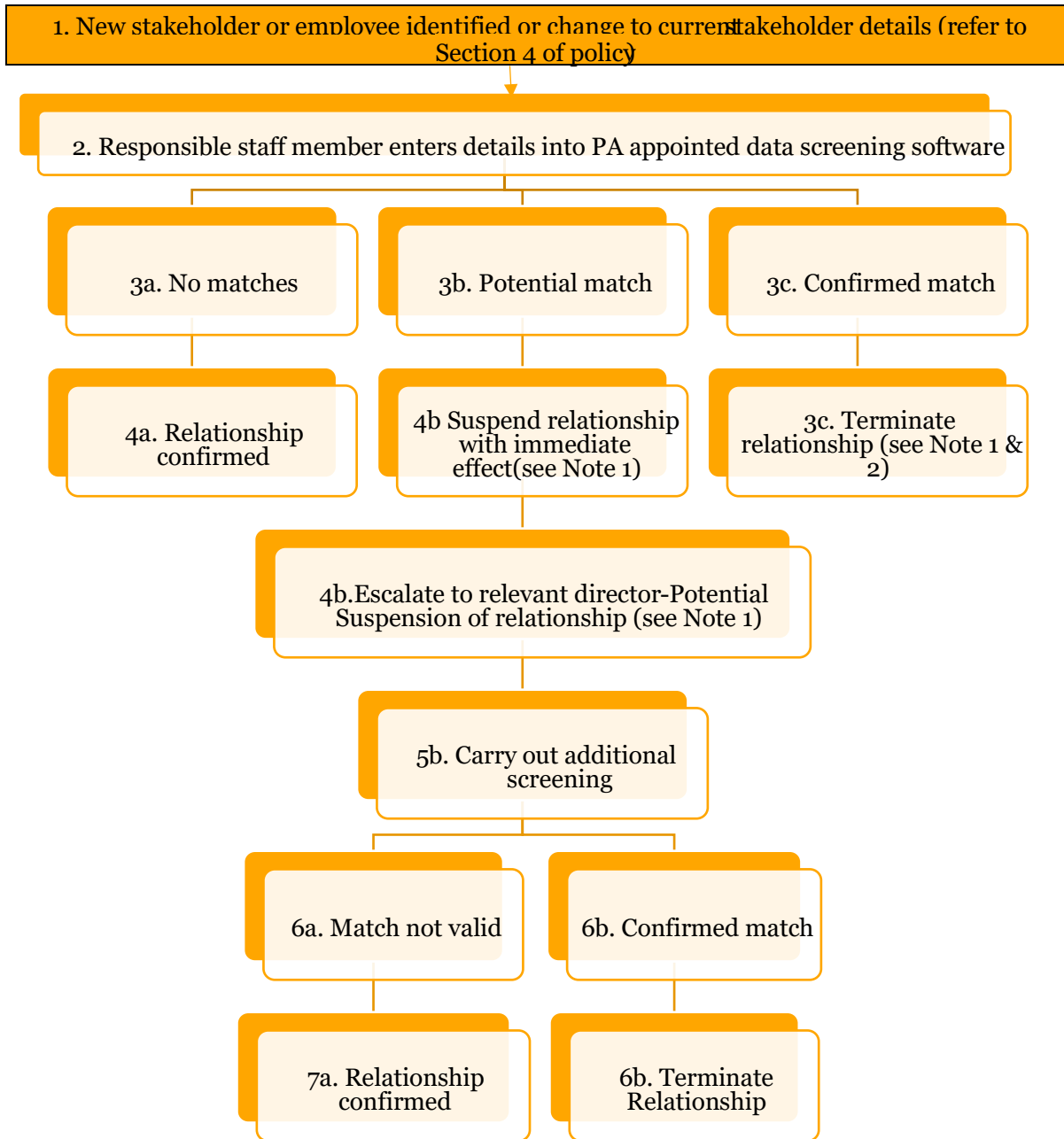
8. Confidentiality

Practical Action is committed to protecting the privacy and security of personal information and all information relating to the screening will be treated confidentially. For the UK based team, the *Privacy Notice* explains how we collect, manage, use and protect personal information. [Privacy Notice - Practical Action](#)

Practical Action processes personal data collected in accordance with our Data Protection policy/Privacy Notice. In particular, data collected as part of the financing terrorism screening process is held securely and accessed by, and disclosed to, individuals only for the purposes of managing either the recruitment exercise effectively and to decide to whom to offer the job. Inappropriate access or disclosure of personal data constitutes a data breach and should be reported in accordance with Practical Action's Data Protection policy/ Privacy Notice immediately. It may also constitute a disciplinary offence, which will be dealt with under the organisations disciplinary process.

9. Appendix

Appendix 1: The Internal Process



Note 1: All confirmed matches must be communicated to the relevant Director and Chief Financial Officer immediately. Suspension or termination of relationships with the affected stakeholders and communication with the relevant donors will be managed by the appropriate Director from the Group Management Team.

Note 2: All external communications relating to terrorist financing must be channelled through the Fundraising, Marketing and Communications Director and be approved by the CEO prior to issue.

Appendix 2: USAID Partner Vetting

- USAID policy directives and required procedures for partner vetting;

[ADS Chapter 319 - Partner Vetting \(usaid.gov\)](#) Jan 2021.

- USAID guidance to support the review and validation of information submitted on USAID Form 500-13, the Partner Information Form (PIF)

[USAID Guidance on the Identification of Key Individuals - A Mandatory Reference for ADS Chapter 319](#) Jan 2021.

- Partner information vetting form;

[AID 500-13 \(Partner Information Form\) | Forms | U.S. Agency for International Development \(usaid.gov\)](#) Jan 2024.

ⁱ Terrorism Act 2000 [Terrorism Act 2000 \(legislation.gov.uk\)](#)

ⁱⁱ European Council Regulation EC/2580/2001 (as amended) [Regulation - 2580/2001 - EN - EUR-Lex \(europa.eu\)](#)

ⁱⁱⁱ Terrorism (United Nations Measures) Orders 2009 of the United Kingdom [The Terrorism \(United Nations Measures\) Order 2009 \(legislation.gov.uk\)](#)