

NON-PROFITS • MEMBER CHECKLIST

NPO Vulnerability Checklist

Protecting your organisation from white-washing and financial crime exploitation. Thirty-seven questions, six sections, one clear risk level.

HOW TO USE THIS CHECKLIST

Non-profits are trusted, which is exactly why they are targeted. Criminals may donate to buy legitimacy, or to “white-wash” a reputation. Work through this checklist with your finance and fundraising teams and tick what is *genuinely* in place.

Organisation name

Registration number

Completed by

Role / title

Date completed

Jurisdiction

1 Donor due diligence

BASIC CHECKS (ALL DONATIONS)

#	Item	Yes	No	N/A
1.1	Do you collect full name and contact details for all donors?	☐	☐	☐
1.2	Do you verify donor identity for donations above a set threshold?	☐	☐	☐
1.3	Do you record the source of funds for significant donations?	☐	☐	☐
1.4	Do you maintain a record of donation history for each donor?	☐	☐	☐

ENHANCED CHECKS (HIGH-VALUE OR UNUSUAL DONATIONS)

#	Item	Yes	No	N/A
1.5	Do you conduct enhanced due diligence above a higher, defined threshold?	☐	☐	☐
1.6	Do you screen donors against publicly available sanctions lists?	☐	☐	☐
1.7	Do you run basic adverse media searches on major donors?	☐	☐	☐
1.8	Do you verify the legitimacy of corporate donors through the official company registry?	☐	☐	☐

2 Red flag detection

Do you have monitoring in place for each of these?

DONATION PATTERNS

#	Red flag	Monitored	Not yet
2.1	Donation size inconsistent with the donor's apparent profile	☐	☐
2.2	Several smaller donations structured to stay under thresholds ("smurfing")	☐	☐
2.3	Corporate donations made from personal bank accounts	☐	☐
2.4	Donations from high-risk jurisdictions with no clear connection to your cause	☐	☐

DONOR BEHAVIOUR

#	Red flag	Monitored	Not yet
2.5	Donor unusually insistent on public recognition or honorary titles	☐	☐
2.6	Donor requests appreciation letters with specific wording (for example, to support an immigration or residency application)	☐	☐
2.7	Donor resistant to providing basic identification or documentation	☐	☐
2.8	Donor asks for an immediate return of the donation or a partial refund	☐	☐

3 Governance & internal controls

POLICIES AND PROCEDURES

#	Item	Yes	No	In progress
3.1	Do you have a written Gift Acceptance Policy?	☐	☐	☐
3.2	Does the policy include criteria for rejecting donations?	☐	☐	☐
3.3	Is there a documented process for escalating suspicious donations?	☐	☐	☐
3.4	Is a named person responsible for donor due diligence?	☐	☐	☐
3.5	Do you have a policy on issuing tax-deductible receipts, where relevant?	☐	☐	☐

BOARD OVERSIGHT

#	Item	Yes	No	In progress
3.6	Is the Board informed of significant donations (above a threshold it sets)?	☐	☐	☐
3.7	Does the Board review and approve the Gift Acceptance Policy annually?	☐	☐	☐
3.8	Can the Board review donations that have been flagged as high-risk?	☐	☐	☐

4 Record-keeping & reporting

#	Item	Yes	No	N/A
4.1	Do you retain donor records for at least the period your regulator requires (commonly five years or more)?	☐	☐	☐
4.2	Are donation records stored securely with access controls?	☐	☐	☐
4.3	Could you retrieve historical donor records quickly if authorities asked?	☐	☐	☐
4.4	Do staff know how to file a suspicious transaction report with your national financial intelligence unit?	☐	☐	☐
4.5	Is there a process to ring-fence questionable donations until they are clarified?	☐	☐	☐

5 Staff awareness & training

#	Item	Yes	No	In progress
5.1	Have fundraising staff been trained on donor red flags?	☐	☐	☐
5.2	Do staff understand “white-washing” and how non-profits can be exploited?	☐	☐	☐
5.3	Is there a clear reporting line for staff to escalate concerns?	☐	☐	☐
5.4	Are staff aware of your charity regulator’s guidance on donor screening?	☐	☐	☐

6 Banking relationship management

#	Item	Yes	No	N/A
6.1	Do you keep open communication with your bank about your activities?	☐	☐	☐
6.2	Can you give your bank documentation of your governance controls on request?	☐	☐	☐
6.3	Do you tell your bank in advance about expected large or unusual donations?	☐	☐	☐
6.4	Have you avoided banking access problems (account closures, restrictions or delays)?	☐	☐	☐

Your score

Yes = 1 point | No = 0 | In progress or N/A = 0.5. For Section 2, score Monitored = 1 and Not yet = 0.

Section	Max	Your score
1 • Donor due diligence	8	
2 • Red flag detection	8	
3 • Governance & internal controls	8	
4 • Record-keeping & reporting	5	
5 • Staff awareness & training	4	
6 • Banking relationship management	4	
Total	37	

Your risk level

Score	Risk level	Recommended action
31-37	Low	Maintain current controls; review annually.
22-30	Moderate	Address gaps within six months; prioritise Sections 2 and 3.
13-21	Elevated	Urgent review needed; consider external advisory support.
0-12	High	Immediate action; engage the Board and seek professional guidance.

Risk level: ☐ Low ☐ Moderate ☐ Elevated ☐ High

NOTES AND PRIORITY ACTIONS

Key resources to identify in your jurisdiction

Write in the local body for each. Regulators, registries and reporting routes differ by country.

Resource to identify	Purpose	Local body / website
Charity regulator	Guidance, advisories and governance codes	
Financial intelligence unit	Filing suspicious transaction reports	
Company registry	Verify corporate donors	
Sanctions lists	Screen donors against designated persons and entities	
Your bank's compliance contact	Escalate large or unusual donations	

Next steps

- 1 Complete this checklist** with your finance and fundraising teams.
- 2 Identify gaps.** Focus on every “No” in Sections 1 to 4.
- 3 Prioritise quick wins.** Staff training and a Gift Acceptance Policy often have the fastest impact.
- 4 Document your controls.** They become evidence of good governance for banks and regulators.
- 5 Review annually.** Threats evolve; your controls should too.

WHY THIS MATTERS

Cases around the world have shown convicted criminals donating substantial sums to well-regarded charities, using philanthropy to gain legitimacy or to support residency applications. Regulators have since urged charities to review historic donor records. Documented controls protect your reputation and your mission.

A practical starting point, not a comprehensive compliance programme. For tailored guidance, contact JFourth Solutions.