BOTANIC GARDENS
CONSERVATION INTERNATIONAL

Anti-Money Laundering Policy

1. Purpose and scope

Botanic Gardens Conservation International (BGCI) is committed to the highest standards of financial integrity in all its activities, including the receipt of donations, grants and other income, and the management of funds across its global plant conservation programmes. Money laundering is the process by which the proceeds of crime are disguised so they appear to come from a legitimate source. This policy sets out our approach to preventing the organisation, knowingly or unknowingly, from being used as a vehicle for money laundering or terrorist financing.

This policy applies to all trustees, employees, volunteers, consultants and contractors, and to all entities and field offices operating under the charity's name or on its behalf, regardless of location.

Regulatory position

Charities such as Botanic Gardens Conservation International are not generally classed as a "relevant person" under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, and are not normally required to register with HMRC for AML supervision purposes. This policy is adopted as good practice, in line with Charity Commission guidance and expectations of funders, donors and regulators, and to manage the genuine money laundering risks the charity faces through international operations, overseas partners and higher-value donations. Trustees should periodically confirm this position, particularly if the charity's activities or income sources change.

BGCI work spans multiple jurisdictions, some of which carry a higher inherent risk of money laundering due to weaker regulatory environments, cash-based economies, or proximity to illicit trade (including, in some cases, the illegal wildlife and plant trade, which BGCI works to counter). BGCI also receives donations from a wide range of individuals, trusts, foundations and corporate partners. Both factors make a clear and well-understood AML policy essential.

2. Definitions

- ***Money laundering***: the process of concealing the origins of money obtained illegally, typically by passing it through a complex sequence of banking transfers or commercial transactions, so that it appears to come from a legitimate source.
- ***Terrorist financing***: providing or collecting funds, by any means, with the intention or knowledge that they will be used to carry out acts of terrorism.
- ***Suspicious activity***: any transaction, donation, or pattern of activity that appears inconsistent with a donor's or partner's known, legitimate source of funds, or which otherwise gives rise to reasonable suspicion.
- ***Due diligence***: the process of verifying the identity of a donor, partner or counterparty and understanding the source and purpose of funds before accepting or transferring them.
- ***Designated person*** / Money Laundering Reporting contact: the Head of Finance, who acts as the BGCI named contact for receiving and assessing internal reports of suspected money laundering.

3. Our commitments

BGCI will:

- Take reasonable steps to know who we are accepting money from, and where appropriate, who we are sending money to.
- Apply enhanced due diligence to higher-risk donations, partners, and jurisdictions, including those identified on relevant UK, EU, UN or FATF sanctions or high-risk country lists.
- Never knowingly accept funds, gifts in kind, or other donations where there is reasonable suspicion that they derive from criminal activity.
- Ensure all staff with financial or donor-facing responsibilities receive periodic training on recognising and reporting money laundering risks.
- Maintain accurate records of donor due diligence and significant transactions in line with our data protection and record-retention obligations.
- Cooperate fully with law enforcement, regulators and banking partners in connection with any investigation.

4. Donor and partner due diligence

Standard due diligence for most donations and partner transactions, standard due diligence is proportionate. This includes confirming the identity of the donor or partner (individual or organisation), recording the source of funds where this is not self-evident (e.g. a payroll donation or standard online card payment), and checking the donor or partner name, where relevant, against current sanctions lists.

Enhanced due diligence must be applied where any of the following apply:

- A single donation, or cumulative donations from one source within a 12-month period, exceed £25,000 (a guideline threshold — see note below).
- The donation is in cash, or in a form that is difficult to trace (e.g. cryptocurrency, bearer instruments, or third-country wire transfers from an unrelated jurisdiction).
- The donor or partner is based in, or funds are routed through, a jurisdiction identified as high-risk by the Financial Action Task Force (FATF) or UK Government.
- The donor wishes to remain anonymous beyond what is operationally normal (note: legitimate anonymous giving is common and not in itself suspicious, but anonymity combined with other risk factors warrants closer review).
- A donor or partner is a Politically Exposed Person (PEP) or closely associated with one.
- Anything about the transaction otherwise looks, feels, or seems unusual given the donor's or partner's profile.

Overseas partners: given BGCI conservation work is delivered through overseas offices, field teams and in-country partner organisations, due diligence extends beyond incoming donations to outgoing payments and partner relationships. Before entering a funding relationship with a new in-country partner, local agent or grantee, the responsible programme lead must complete a partner due diligence check covering legal status, ownership/control where relevant, banking arrangements, and any sanctions exposure. This sits alongside, and should be read together with, the due diligence requirements in the Anti-Fraud, Bribery and Corruption Policy.

5. Red flags: recognising suspicious activity

Staff and volunteers should be alert to the following indicators, which may (individually or in combination) suggest a heightened money laundering risk. No single factor is automatically suspicious — judgement should be applied in context.

- A donor insists on cash donations significantly above what is typical for our supporter base or repeatedly offers to split a large donation into smaller amounts.
- A donor or partner is reluctant to provide basic identifying information or provides information that is inconsistent or cannot be verified.
- Funds are offered with conditions that seem designed to obscure the origin or true beneficiary of the gift.
- A donation is offered, then the donor asks for some or all of it to be returned or redirected to a third party shortly afterwards.
- Payment instructions for grants or partner payments are changed at short notice, especially to an account in a different country or name than expected.
- A field partner or agent requests payment in cash, to a personal account, or to an account in a third country unconnected to the programme.
- Donations or grant funds appear disproportionate to the known financial standing of the donor or partner organisation.

6. Sanctions screening

BGCI will screen significant donors, grant recipients, overseas partners and suppliers against the UK Office of Financial Sanctions Implementation (OFSI) consolidated list, and other relevant UN, EU or US sanctions lists where BGCI international operations make this appropriate, before entering into a financial relationship and on a periodic basis thereafter. No funds may be accepted from, or transferred to, a sanctioned individual or entity, and any potential match must be escalated immediately. See the BGCI Financial Sanctions policy.

7. Reporting suspicious activity

Any trustee, employee, volunteer, consultant or contractor who becomes aware of, or suspects, money laundering or terrorist financing activity must report this promptly. Reports should be made to the Head of Finance, who acts as the charity's designated contact for this purpose.

Where the concern relates to, or implicates, the Head of Finance, or where the reporting individual does not feel able to report through the usual route, the matter should be escalated directly to the Secretary General or the Chair of the Board of Trustees.

Full details of how to report, what happens after a report is made, escalation routes, confidentiality protections, and the charity's obligations to consider reporting to the National Crime Agency (NCA) are set out in the separate Financial Crime Reporting Procedure, which applies to this policy and to the Anti-Fraud, Bribery and Corruption Policy alike.

Staff must never attempt to investigate suspected money laundering themselves, alert the person(s) concerned ("tipping off"), or take any action that might prejudice a future investigation. Tipping off a person that they are, or may be, the subject of a money laundering investigation or report is a criminal offence.

8. Roles and responsibilities

Role	Responsibility
Secretary General	Overall ownership of this policy; approves and reviews it; receives escalated reports; ensures adequate resources for compliance.
Head of Finance	Day-to-day policy owner; receives and assesses internal reports; leads due diligence on higher-risk donations and partners; maintains records; liaises with banks, auditors and authorities as needed.
Director of Operations	Ensures due diligence and sanctions screening processes are embedded in overseas field programmes and partner agreements; supports the Head of Finance on in-country risk matters.
All staff, volunteers and contractors	Complete required training; apply due diligence procedures relevant to their role; report concerns promptly and do not attempt to investigate independently.

9. Training and awareness

All staff with finance, fundraising, grant-management or partner-facing responsibilities will receive AML awareness training upon induction and at least every two years thereafter. Training will cover how to recognise red flags, the due diligence procedures in this policy, and how to report concerns.

10. Record keeping

Records relating to donor and partner due diligence, sanctions screening checks, and any internal reports made under this policy will be retained for a minimum of five years from the end of the relevant relationship or transaction, in a manner consistent with the BGCI data protection policy and UK GDPR obligations.

11. Related policies

- Anti-Fraud, Bribery and Corruption Policy
- Financial Crime Reporting Procedure
- Whistleblowing Policy
- Data Protection Policy
- Financial Sanctions Policy

12. Policy Review

This policy will be reviewed by the Secretary General at least every two years, or sooner if there is a significant change in the BGCI risk profile, a relevant change in law or regulation, or following any incident that highlights a gap in this policy.

Policy version:	v02
Last revision date:	June 2026
Next review date:	Every 2 years, or sooner following a significant incident or regulatory change
Policy owner:	Head of Finance
Created by:	Anne-Marie Frankland
Authorised by:	Secretary General