The Global Biodiversity Standard

Anti-Fraud, Bribery and Corruption Policy

October 2026

Status	Approved and in force
Version	1.1
Policy owner	CEO, with Board oversight
Approved by	TGBS Ltd Board of Directors
Approval date	21 October 2026
Effective date	21 October 2026
Next review	October 2027: Annually, and after any material incident or legal change

The Global Biodiversity Standard (TGBS Ltd)

Anti-Fraud, Bribery and Corruption Policy

TGBS Ltd company policy

TGBS has zero tolerance for fraud, bribery, corruption and money laundering. Controls will be proportionate to a small international company, but every allegation will have an independent escalation route and a documented response.

1. Purpose

This policy protects TGBS funds, assets, certification integrity, data and reputation. It establishes proportionate prevention, reporting, investigation and recovery arrangements suited to TGBS's present size and operating model.

- TGBS will act honestly, transparently and in the best interests of the company and its mission.
- No person may commit, facilitate, conceal or benefit from fraud, bribery, corruption or associated financial crime on behalf of TGBS or a client.
- Prevention controls will be risk-based and proportionate to TGBS size, resources, countries of operation and delivery model.
- Commercial pressure, local custom, urgency or an instruction from a senior person never excuses misconduct.

2. Scope

This policy applies to TGBS Ltd directors, officers, employees, workers, consultants, contractors, volunteers and interns. It also applies, to the extent stated in contract or appointment terms, to TGBS hubs, certified assessors, technical reviewers, committee members, delivery partners and any other person acting for or representing TGBS.

2.1 Key terms

- **Fraud:** dishonest conduct intended to make a gain, cause a loss or expose another to a risk of loss, including false representation, failure to disclose, abuse of position, false accounting and misuse of certification or project evidence.
- **Bribery:** offering, promising, giving, requesting or accepting an advantage to induce or reward improper performance. It includes bribery of public officials and bribes paid through an intermediary.
- **Corruption:** abuse of entrusted power for private or organisational gain, including kickbacks, collusion, nepotism used to distort a decision and undisclosed conflicts.
- **Facilitation payment:** an unofficial payment intended to secure or speed up a routine action. TGBS prohibits these, except where a person reasonably believes payment is necessary to protect life, liberty or immediate safety; any such payment must be reported as soon as safe.

- **Associated person:** anyone performing services for or on behalf of TGBS, which may include hubs, assessors, agents or subcontractors depending on the circumstances.

3. Policy principles

TGBS will apply this policy lawfully, fairly, consistently and proportionately, with effective oversight, documented decisions and protection from retaliation.

4. Roles and responsibilities

- The Board approves the policy, oversees material risks and ensures that allegations involving senior leadership are handled independently.
- The CEO implements the policy, assigns proportionate controls and reports material matters to the Board. A responsibility may be delegated, but accountability remains with the role that delegated it.
- Directors and managers model the required conduct, act on concerns promptly, protect reporters from retaliation and identify conflicts before taking part in a decision.
- All covered persons must understand the policy, keep accurate records and raise concerns without delay.
- Each hub must nominate a responsible lead, cascade relevant requirements to assessors and subcontractors, maintain suitable local controls, comply with applicable local law, and report material concerns to TGBS. A hub remains responsible for its own legal duties and personnel.
- Assessors and reviewers must act impartially, declare conflicts, protect evidence and information, and never allow commercial or relationship pressures to affect their professional judgement.
- The person responsible for finance will maintain core payment, reconciliation, expense and asset controls and notify the CEO and a non-conflicted director of unexplained exceptions.
- The Board may appoint an external investigator, accountant or lawyer for a specific matter; this does not create a permanent counter-fraud function.

5. Policy requirements

5.1. Risk assessment and financial controls

- Review fraud and bribery risks at least annually and before entering a high-risk country, funding arrangement, major contract or new hub relationship.
- Use written authority limits, documented budgets, independent review and separation of request, approval and payment wherever practicable. Where staffing prevents full separation, a director must perform a documented compensating review.
- Make payments only against valid documentation to verified accounts in the counterparty's name. Changes to bank details require independent confirmation through a known channel.
- Reconcile bank and accounting records regularly; review unusual journal entries, refunds, discounts, write-offs and duplicate or split payments.
- Run proportionate counterparty due diligence and sanctions screening under this policy, the Counter-Terrorist Financing Policy and the Financial and Counterparty Due Diligence Policy.

5.2. Certification and project integrity

- Assessment evidence, scores, reviews, certificates, invoices and funder reports must be complete, accurate, traceable and not misleading.
- Assessors, hubs and reviewers must declare conflicts and must not alter findings to obtain certification, satisfy a client, protect revenue or benefit TGBS.
- TGBS marks, certificates and claims may be used only as authorised. Suspected falsification or misuse must be reported promptly.

5.3. Gifts, hospitality and expenses

Reasonable relationship-building and culturally appropriate hospitality may be permitted, but it must be lawful, transparent and never influence - or appear to influence - a decision. The following thresholds apply consistently across TGBS policies:

Value or circumstance	Required action
Cash, cash equivalents, personal discounts, loans, kickbacks or anything offered to influence a decision	Never offer, solicit or accept, regardless of value.
Up to £50 for a single modest gift or hospitality item	May be accepted or offered only when lawful, infrequent, transparent, not connected to a live procurement/certification decision and incapable of creating an obligation. Record it if there is any doubt.
More than £50 for one item, or more than £150 in aggregate from/to the same source in a rolling 12 months	Declare in the Gifts and Hospitality Register within five working days and obtain prior written approval from the CEO where practicable. If the CEO is involved, approval must come from the Chair or another non-conflicted director.
More than £150 for one item; travel or accommodation; or hospitality involving a public official	Prior written approval from the CEO. If the CEO is involved, approval must come from the Chair or another non-conflicted director.
A culturally significant gift that would cause offence to refuse	Accept on behalf of TGBS, declare promptly, and agree whether it will be retained by TGBS, displayed, shared or donated. It must never affect a decision.

Amounts are assessed at fair market value and converted to pounds sterling at the date of offer. Splitting, repeated low-value items and benefits given to family members are aggregated. The CEO maintains the register and the Chair reviews entries involving the CEO.

5.4. Political and charitable contributions

TGBS funds must not be used for party-political contributions. A donation or sponsorship may be made only for a legitimate, documented purpose aligned with TGBS objectives, following due diligence and approval under delegated authority. It must not be used as a disguised bribe.

5.5. Terrorist financing

TGBS will not accept, move or distribute funds where it knows or reasonably suspects that assets support terrorism. Detailed bank-facing controls are set out in the separate Counter-Terrorist Financing Policy.

5.6. Anti-money laundering controls

TGBS is not a business in the UK regulated sector. It will nevertheless apply proportionate anti-money-laundering controls because it receives fees, grants and other funds and works through international partners and hubs. If an activity brings TGBS within a regulated regime, the stricter legal requirements will apply.

5.7. Definitions and responsibility

- **Money laundering:** concealing, disguising, converting, transferring, removing, acquiring, using or possessing criminal property, or becoming involved in an arrangement that facilitates it.
- **Criminal property:** property that represents a benefit from criminal conduct where the person knows or suspects that fact.
- **Beneficial owner:** the individual who ultimately owns or controls an entity or on whose behalf a transaction is conducted.
- **Politically Exposed Person (PEP):** a politically exposed person, including relevant family members and close associates. PEP status is a risk factor, not evidence of wrongdoing.
- **Enhanced due diligence:** additional checks and senior approval applied where risk is higher.

The CEO acts as Compliance Lead unless the Board designates another competent person. This is an internal governance role and does not assert that TGBS must appoint a statutory Money Laundering Reporting Officer. Finance personnel must verify payer and payee details, monitor exceptions and stop a transaction when required checks are incomplete.

5.8. Standard due diligence

- Verify legal name, registration, address, authorised representative, bank account and beneficial ownership using reliable, independent information.
- Understand the relationship, services, source and intended use of funds and expected payer, amount, timing and destination.
- Screen relevant entities and individuals against UK sanctions and any other lists legally applicable to the transaction.
- Confirm that contract, invoice and payment details match and that services are plausible and evidenced.
- Do not accept anonymity, unexplained third-party payments or structures that obscure control, source or destination of funds.

5.9. Enhanced due diligence and red flags

Enhanced due diligence and written approval from the Compliance Lead and a non-conflicted director are required where risk is high, including:

- a high-risk or sanctioned jurisdiction, PEP, credible adverse information or opaque ownership structure;
- a request for cash, cryptocurrency, secrecy, an overpayment or refund, split transactions or payment through an unrelated third party;
- funds inconsistent with the counterparty's activities, an unexplained change of bank account or reluctance to provide information;
- a large or unusual transaction, complex funding chain, subgranting or transfer to an individual account;
- a counterparty that is newly formed, dormant, unverifiable or using nominee arrangements without a clear legitimate rationale.

TGBS will not accept anonymous cash or cryptocurrency. Cash payments above £250 require exceptional prior written approval, identification of the payer, a documented legitimate reason and a receipt. Normal payments must use traceable banking channels.

5.10. Monitoring and suspicious activity

- Refresh checks when ownership, bank details, jurisdiction, purpose or risk changes and at least annually for high-risk relationships.
- Compare actual payments and delivery with the expected profile and investigate material variances, refunds and onward transfers.
- Do not proceed, return funds or alert the counterparty if doing so could prejudice a lawful enquiry. Seek legal or banking advice promptly.
- The Compliance Lead will consider whether a report to the National Crime Agency, police, bank, regulator or other competent authority is required or appropriate.

6. Reporting and escalation

A person may raise a concern orally or in writing and may be accompanied or supported where appropriate. Anonymous reports will be considered as far as the available information allows. Reports should include the facts known, relevant dates, people involved and any evidence that can be preserved safely.

Situation	Route
Ordinary route	Report to the CEO and copy the Board Chair or another non-conflicted director.
Concern involves the CEO	Report to the Board Chair and at least one other non-conflicted director. The CEO must not receive, direct or decide the matter.
Concern involves the Board Chair	Report to the CEO and at least one other non-conflicted director. The Chair must not receive, direct or decide the matter.
Concern involves both the CEO and Chair, several directors, or internal independence is reasonably in doubt	Report to any non-conflicted director or to the Governance Contact, who must notify at least one other non-conflicted director and arrange an independent response. External professional advice or an external investigator must be used where necessary.
Immediate danger or suspected crime/regulatory breach	Contact emergency services, law enforcement or the relevant regulator where appropriate. Internal reporting is not a precondition.

The Board will maintain a current Policy Contact Register containing direct contact details for the CEO, Chair, Governance Contact and at least two other directors. The Governance Contact means the Company Secretary, if appointed, or a non-conflicted director designated by the Board.

No person may investigate, influence, decide or hear a review of a matter in which they are implicated or have an actual, potential or perceived conflict of interest. A report received by an implicated person must be forwarded immediately to a non-conflicted route without screening or alteration.

Retaliation, victimisation, obstruction, concealment, destruction of evidence and knowingly false or malicious allegations are prohibited. A report made honestly will not attract action merely because it is unsubstantiated.

The initial recipient must secure records, avoid alerting a suspected person where that could prejudice enquiries, assess immediate financial or safety risks and notify a second non-conflicted decision-maker. No one should conduct covert searches, interview suspects or promise an outcome without authority.

The CEO and non-conflicted director will agree a proportionate response plan covering independence, evidence, data protection, insurer/funder/bank notifications, legal advice, law-enforcement or regulator reporting, recovery of funds and communications. Where either is implicated, the alternative route in the table applies.

7. Response and resolution

1. Triage promptly and document the decision to investigate, refer, monitor or close, with reasons.
2. Use an investigator who is competent and independent of the events and decision-makers. Serious or senior-level allegations should normally be investigated externally.
3. Give affected persons a fair opportunity to respond, subject to evidence preservation, legal restrictions and safety considerations.
4. Report substantiated loss, control failures and remedial actions to the Board. Material incidents must be notified to funders, banks, insurers, regulators or law enforcement where legally or contractually required.
5. Recover losses where proportionate and correct affected certification decisions, reports or public claims.

8. Confidentiality and records

Information will be shared only with those who need it to protect people, assess the matter, comply with law, obtain advice or take action. Absolute confidentiality cannot be promised where disclosure is necessary for a fair process or legal duty.

Fraud risk assessments, approvals, the Gifts and Hospitality Register, due-diligence records and investigation files will normally be retained for at least six years, subject to legal advice, limitation periods and the TGBS retention schedule.

Personal data will be handled under the TGBS Data Protection Policy. Records must be factual, access-controlled and kept separately from general personnel or project files where sensitivity requires it.

9. Breaches and corrective action

A breach may result in corrective action, removal from an assignment, disciplinary or contractual action, suspension or termination of a hub or assessor relationship, recovery of losses, and referral to law enforcement or a regulator where appropriate.

10. Monitoring and review

The CEO will review controls annually using the principles of top-level commitment, risk assessment, proportionate procedures, due diligence, communication and monitoring. The Board will receive an anonymised summary of reports, losses, gifts above threshold and remedial actions.

11. Related documents and legal framework

- TGBS Code of Conduct; Whistleblowing Policy; Conflicts of Interest Policy.
- TGBS Counter-Terrorist Financing Policy; Financial and Counterparty Due Diligence Policy.
- Fraud Act 2006; Bribery Act 2010; Theft Act 1968; Companies Act 2006; Criminal Finances Act 2017; Economic Crime and Corporate Transparency Act 2023; Proceeds of Crime Act 2002; Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, where applicable; Sanctions and Anti-Money Laundering Act 2018.