

Anti-Money Laundering and Fraud Prevention Policy

GreenSpark will take reasonable, risk-based steps to prevent and detect fraud, money laundering, terrorist financing, tax evasion facilitation and other financial misconduct relevant to its activities.

Status: Final — Approved and Published **Version:** 1.0

Approved: 1 July 2026 **Published:** 1 July 2026

Policy owner: GreenSpark Consulting — Management **Next review:** 1 July 2027

Policy statement

GreenSpark will take reasonable, risk-based steps to prevent and detect fraud, money laundering, terrorist financing, tax evasion facilitation and other financial misconduct relevant to its activities.

1. Scope and limitations

Applies to client onboarding, project finance support, supplier payments, commissions, reimbursements and other commercial or financial transactions.

Specific statutory anti-money-laundering duties depend on the activities performed and whether GreenSpark falls within a regulated sector. This policy does not by itself determine that status.

2. Minimum controls

- Use proportionate identity, ownership and business-purpose checks where risk warrants.
- Keep accurate records. False invoices, backdated contracts, misleading service descriptions and off-book transactions are prohibited.
- Do not knowingly help disguise the origin, ownership, destination or purpose of criminal proceeds or facilitate tax evasion.
- Do not accept unexplained overpayments, split payments, unusual third-party payments or requests to return funds to a different account without investigation.

3. Payment and invoice controls

- Verify counterparties and bank-account details through reliable independent channels, especially when payment instructions change.

Where practicable, use segregation of duties or a second-person check for material payments and changes to payment instructions.

Confirm invoices match contracts, approved purchase orders and delivered work.

- Apply additional checks to complex cross-border structures, opaque ownership, high-risk jurisdictions or unusual funding routes.

4. Suspicion and escalation

- Pause suspicious payments or transactions where lawful and operationally appropriate.

Preserve records and report concerns to the designated compliance lead or an independent director. Avoid tipping off where legal restrictions apply.

- Assess whether specialist advice, a report to an appropriate authority or other action is required. Document the rationale for proceeding, rejecting or escalating.

5. Responsibilities and review

Finance or the nominated payment approver verifies supporting evidence and approvals. Project leads validate delivery and commercial rationale. All covered persons must report suspected fraud, altered bank details, invoice manipulation or unexplained payment requests.

- Retain due-diligence evidence, contracts, invoices, payment approvals, bank-detail verification, exception logs and investigation records under the retention schedule.

Review annually and after a material incident or change in services or risk.

Related guidance

Seek legal advice where regulated-sector AML obligations, suspicious activity reporting or other formal duties may apply.

Approval and document control

This is the published version 1.0 of this policy, with approval and publication dates recorded as 1 July 2026. It forms part of the GreenSpark Consulting — Governance, Integrity & Responsible Business framework and should be read with other relevant policies and applicable law.

Approved status: Approved **Effective date:** 1 July 2026 **Review date:** 1 July 2027