Fraud prevention and detection and anti-money laundering policy

This policy sets out the responsibilities for the prevention of fraud and outlines the actions to be taken if fraud is suspected or discovered.

The term fraud, when used in this document, means actual fraud, attempted fraud or suspected fraud, at whatever level or location, or of whatever level of significance.

Directors and staff are required at all times to act honestly and with integrity and to safeguard the resources for which they are responsible. Fraud is an ever-present threat to these resources and hence must be a concern of all directors and members of staff.

The Company takes seriously any attempt to commit fraud by directors, members of staff, contractors, their employees and agents. Directors or staff involved in impropriety of any kind will be subject to disciplinary action, including prosecution, if appropriate. The Company treats attempted fraud as seriously as accomplished fraud.

Specific guidance on the identification and reporting of money laundering is included at the end of this document.

This policy should also be considered alongside the Company's "Ethical and anti-corruption policy" (PO-001) and the associated guidance (GD-001).

What is fraud?

Offences generally referred to as fraud are covered by a range of legislation; for the Company's purposes fraud is defined as the intention or attempt (be it successful or not) to gain an advantage, avoid an obligation or cause loss dishonestly through falsification of records or documents by a director or a member of staff or an external person.

For the purposes of this policy, the following are also considered fraudulent activities (this list is not exhaustive): deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, abuse of position, false representation, concealment of material facts and collusion.

The term applies to physical assets as well as data and intellectual property. It also includes the use of information technology equipment to manipulate programs or data dishonestly, the theft of IT equipment and software, and the intentional misuse of computer time and resources.

Responsibilities

Directors and staff must:

- act with propriety in the use of the Company's resources and the handling and use of funds;
- conduct themselves with integrity, objectivity, accountability, openness, and honesty;
- follow codes of conduct, including policies on gifts and hospitality;
- alert their line manager where they believe the opportunity for fraud exists because of poor procedures or lack of effective supervision;
- alert their line manager or other responsible person if they know or suspect a fraud may be happening;
- develop and maintain effective controls to help prevent or detect fraud; and
- assist in any investigations by making available all relevant information and by co-operating in interviews.

Line managers have additional responsibilities to:

- ensure that an adequate system of internal control exists within their areas of responsibility;
- ensure controls operate effectively;
- identify and assess the risks involved in the operations for which they are responsible;
- develop and maintain effective controls to prevent and detect fraud;
- diligently perform any tasks intended to minimize potential fraud;
- ensure their staff comply with the requirements for reporting any instances of fraud; and
- report suspected or actual fraud immediately as set out below.

Procedures

Reporting fraud

It is the duty of every director and member of staff to report any instance of fraud immediately.

The details of the fraud must be reported to their line manager and to the Chief Financial Officer. If the disclosure concerns any of these individuals, it must be referred upwards to their line manager – and so on up to the Chair of the Group Board of Directors. The risk of duplicity should be considered at all times in terms of determining the reporting group.

The details should include:

- the location involved;
- the amount of potential loss to the Company;
- the amount of any actual loss to the Company;
- details of how the potential/actual loss occurred;
- any actions already initiated; and
- any other relevant details to enable the seriousness of the incident to be assessed.

Staff should not be afraid of raising concerns. The Public Interest Disclosure Act provides protection for employees who raise reasonable concerns through the appropriate channels (see also the whistle blowing policy). Staff will not suffer discrimination or victimisation as a result of following these procedures and the matter will be treated sensitively and confidentially.

The Chief Financial Officer will, in conjunction with Personnel or Legal colleagues as appropriate:

- carry out vigorous and prompt investigations;
- take disciplinary and/or legal action against the perpetrators of the fraud;
- take disciplinary action against managers where their failures have contributed to the commission of the fraud.

It is the responsibility of the Chief Financial Officer to inform the Chief Executive and Chair of the Group Board of Directors.

Response procedure

All incidents will be investigated by appropriate members of the Finance, Legal or Personnel Teams. The Head of Legal and/or an external investigator will become involved as required. The outcome of the investigation will determine what action should be taken which will depend on:

- the weaknesses of internal control systems;
- whether it could be replicated elsewhere in the Company; and
- the level of impact on the Company's reputation.

The actions to be taken will be influenced by the Chief Financial Officer who will, as appropriate:

- monitor progress of any investigation to its conclusion, satisfactory resolution, and determination of resultant action(s), and completion of a written report on the incident, if significant;
- involve the Chief Executive, if the Company's reputation may be implicated;
- instigate further investigation/action;
- ensure appropriate communication with the Police and any other legal or regulatory bodies including external auditors is actioned; and
- determine whether to make an insurance claim.

Rules of evidence

Any investigation involving an employee will be carried out in line with the established Disciplinary Policy and Procedure, but will also be conducted with due regard to rules of evidence and any possible future criminal or civil actions. These include that the employee involved:

- is entitled to know the nature of the allegations against them, or the suspicions;
- is entitled to have a representative present at any interview, who may speak on their behalf;
- is given the opportunity to state their case; and
- is entitled to know the outcome of the investigation into the incident.

Anti-money laundering

Policy

The Company fully supports UK and other governments' initiatives in the fight against crime, terrorism and terrorist financing and associated money laundering activities. This document sets out the Company's policies, procedures and controls to be adopted to ensure that its statutory obligations are met.

Definition of money laundering and how could it affect the Company

Legislation covering money laundering includes:

- the Proceeds of Crime Act 2002;
- the Money Laundering Regulations 2003;
- the Terrorism Acts 2000 and 2002;
- the Drug Trafficking Act 1994;
- the Anti-terrorism, Crime and Security Act 2001; and
- the Criminal Finances Act 2017.

The National Criminal Intelligence Service (NCIS) defines money laundering as:

"The process of moving illegally generated funds through a cycle of transformation in order to create the end appearance of legitimately earned funds."

Thus, it should be noted that a money launderer's prime objective is to disguise the origin of criminal funds and not necessarily to make a profit - so a launderer may well be prepared to undertake transactions at a financial loss.

The need for, and ability of, criminals to invent new ways of laundering funds is high. New techniques and approaches are constantly being used, and are therefore difficult to predict and identify. However, the key risk areas of activity where unusual offers and/or requests should ring alarm bells could be:

- a transaction or business partner based in a country known for widespread corruption;
- refusal by a client or customer to confirm its compliance with applicable anti-corruption laws;
- failure to respond adequately to any question raised by the Company as part of its pre-contract due diligence enquiries;
- recommendation of a business partner by, or ties of a business partner with, public or government officials;
- any transaction involving or requesting a significant sum of cash payments, upfront payments, contingency or 'success' fees;
- excessive or unusually high fees, commission or even volume discounts as compared with normal market expectations;
- receipt of a major donation, gift-in-kind or sum of monies, followed by a request for repayment (or partial repayment) to the donor or another party - for whatever reason;
- an offer from a dubious source to purchase a charity property, or other major asset;
- a communication from, or proposal or request to deal with a foreign or overseas based entity whose authenticity, legitimacy or connection to an existing client or customer is not fully clear;

- dubious requests of any sort for significant payments or payment to be made to an unusual / third party account, PO Box account or to a bank located in a different country from the entity requesting payment; or
- a lack of or unwillingness to provide appropriate documentation supporting a payment request.

General company controls and reporting

The key general controls against money laundering are that the Company and its subsidiaries:

- has segregated controls over receipts and payments;
- requires an awareness among directors, managers and employees of the money laundering possibility, and that this policy is published on the Company's intranet;
- flags on sanctioned countries in the Corporate Database and facilities to run checks on proposed customers and controlling parties;
- places a duty on each director, manager and employee, particularly all authorised signatories, to consider and question any receipt, payment or business proposal of a dubious or uncommon or unusual nature in the light of money laundering possibilities, and requires them to report any such suspicion or concern immediately to their Director.

Following any such report, the Company's established fraud reporting, recording and response procedures outlined above should be followed.

This policy is communicated to all staff via the company intranet. New staff are introduced to the policy on induction.

Ridha Bentiba
Executive Director, HR Wallingford Ltd

Signed: 

Date: 09 April 2024

Review date: 09 April 2025