ANTI-FINANCIAL CRIME POLICY

Policy Statement Summary	The Anti-Financial Crime Policy describes the general framework established by the FIA Foundation (Foundation) for its approach tor managing Financial Crime risk and compliance with the applicable laws and regulations.
Scope	This policy applies to Foundation trustees, employees, agents, consultants, and anyone representing the Foundation. It replaces and supplements the Foundation's previous Anti-Bribery and Corruption Policy and Anti-Fraud Policy and Fraud Response Plan.
Approval Type	Board of Trustees
Review cycle	Annual
Version Number	1
Owner	Company Secretary
Approver	Board of Trustees
Approved Date	22 October 2025
Last Revision Date	n/a
Effective Date	22 October 2025

1. **PURPOSE**

This Anti-Financial Crime Policy:

- outlines the FIA Foundation's (Foundation) approach to achieving our anti-financial crime objectives;
- provides guidance on how to recognise and address financial crime issues; and
- defines the conduct standards that we must all meet to ensure compliance with relevant laws and regulation.

2. **WHO IS RESPONSIBLE FOR THIS POLICY?**

The Board of Trustees has overall responsibility for ensuring the Anti-Financial Crime Policy complies with the Foundation's legal and ethical obligations, and that all those under our control comply with it.

The Director of Partnerships (for programmes questions) and the Company Secretary (for all other questions) have primary and day-to-day responsibility for implementing this Policy, monitoring its use and effectiveness, and dealing with any queries on its interpretation.

Management at all levels are responsible for ensuring those reporting to them are aware of and understand this policy and are given adequate and regular training on it.

3. **WHO IS COVERED BY THIS ANTI-FINANCIAL CRIME POLICY?**

This Anti-Financial Crime Policy applies to all individuals working within the Foundation as trustees, employees, agents, consultants, or other person who may represent the Foundation. It is also provided to partners, grant recipients, and associates, who are required to take reasonable steps to ensure that, in carrying out activities supported by the Foundation, they and their directors, officers, employees and associates must ensure compliance with this Policy and all applicable laws and regulations.

In this policy, "third-party" means any individual or organisation you come into contact with during the course of your role.

4. **YOUR RESPONSIBILITIES**

You should read, understand, and comply with this policy. Importantly, you must report any suspected breaches of this policy to your line manager as soon as you become aware of them.

If, in the course of your employment or association with the Foundation, you become aware of or suspicion of financial crime, you should **report this immediately** to the Company Secretary.

The Foundation considers a breach of this policy to be a serious violation which may result in disciplinary measures, including the dismissal of employees or the termination of its business relationship with any third party. A breach of this policy may also put you and the Foundation at risk of committing criminal offences.

5. WHAT IS FINANCIAL CRIME?

Financial crime is any kind of criminal activity that creates a financial or monetary gain. It includes, but is not limited to, fraud, theft, tax evasion, money laundering, terrorist financing, bribery, and corruption. Financial crime can be committed by individuals or corporations.

Fraud involves dishonesty to gain an unfair or unlawful advantage. This can be through false representation, failing to disclose information, or abusing a position of trust to make a gain or cause a loss;

Tax evasion is a deliberate attempt not to pay tax that is due;

Money laundering is the process of concealing the origins of illegally obtained money. It aims to make the proceeds of crime appear legitimate;

Terrorist financing involves the provision of funds or financial support to individuals or groups engaged in terrorist activities. This can include the collection, movement, and use of funds to support terrorism;

Bribery involves offering, promising, or giving anything of value to induce the improper performance of a function or activity. Bribes can take many forms, including money, gifts, kickbacks, loans, fees, hospitality, services, discounts, charitable contributions, contracts, or votes; and

Corruption is the misuse of power for private gain, whether in public office or business. It diverts money and other resources from those who need them most, hinders economic and social development, and damages business by increasing the cost of goods and services.

6. OUR APPROACH TO FINANCIAL CRIME

The Foundation takes a zero-tolerance approach to Financial Crimes and will actively uphold all applicable laws relevant to countering any involvement in Financial Crime in all the jurisdictions in which it operates.

7. RISK ASSESSMENT, MONITORING AND REVIEW

This Anti-Financial Crime Policy has been developed so that the requirements are proportionate to the risks we face. We have established the risks by performing an assessment of the risk of our organisation being exposed to Financial Crime. We keep this assessment under regular review and will make appropriate changes to our policies as necessary.

The Board of Trustees annually assess the policies' effectiveness. Our Compliance Officers will monitor and oversee our control systems to ensure they deter financial crime.

The Executive Director is responsible for ensuring that third parties who carry out activities supported by the Foundation understand the requirements of this policy.

8. WHAT SHOULD YOU DO IF YOU THINK SOMETHING IS WRONG?

You **must speak out** if you discover or suspect anything wrong, corrupt or otherwise improper occurring in relation to our work as a Foundation. This is essential to our maintaining integrity in what we do as a Foundation.

If you discover or suspect financial crime, whether by:

- another staff member;
- a third party who represents us;
- one of our suppliers or competitors; or
- anyone else in the course of your work,

you **must report this immediately** to your line manager or the Company Secretary. It is important that you raise any concerns you may have early. You may be required to explain any delays.

9. CONSEQUENCES FOR BREACHING THIS POLICY

The Foundation will not tolerate financial crime of any kind. The consequences of committing any of the financial crimes covered by the policy cannot be overstated:

- individuals can be sentenced to long prison sentences;
- the Foundation could be liable to pay significant financial penalties;
- the Foundation may incur significant financial losses; and
- immeasurable reputational damage.

Failing to comply with this policy, and related procedures, could weaken our financial crime prevention framework and thereby leave the Foundation vulnerable to committing or falling victim to financial crimes.

As such, the Foundation takes compliance with this policy and related procedures very seriously. Failure to comply with any requirement of this policy may lead to disciplinary action dismissal for gross misconduct. Any non-employee who breaches this policy is liable to have their contract terminated with immediate effect.

Individuals not complying with this policy may also commit a criminal offence and put the Foundation at risk of committing criminal offences.

10. RESPONDING TO CONCERNS AND CONFIDENTIALITY

The Foundation is committed to ensuring that all internal reports about financial crime concerns will be dealt with appropriately, consistently, fairly and professionally.

All concerns raised will be treated in confidence and every effort will be made not to reveal the identity of an individual who raises a concern if that is their wish. If disciplinary or other proceedings follow the investigation, it may not be possible to take appropriate action as a result of a disclosure without the help of the individual who raised the concern. In those circumstances, the individual may be asked voluntarily to come forward as a witness. If they agree to this, they will be offered advice and support.

11. TRAINING AND COMMUNICATION

All employees will receive periodic training on our Anti-Financial Crime Policy. Training should also be available to trustees, consultants, and relevant agents.

Employees required to undergo training on this Policy should complete a periodic certification that they (a) have completed and understood the required training, (b) have complied with this Policy in the past, and (c) agree to comply with this Policy in the future.

The Foundation's zero-tolerance approach to financial crime will be communicated to everyone covered by the Policy.

12. RECORD KEEPING

The Foundation must keep financial records for six years and have appropriate internal controls in place which will evidence the business reason for making payments to third parties. You must ensure all expenses claims relating to hospitality, gifts or expenses incurred to third parties are submitted in accordance with the Foundation's expenses policy, Anti-Bribery and Corruption Policy and Gifts and Hospitality Policy and specifically record the reason for the expenditure.

All accounts, invoices, memoranda and other documents and records relating to dealings with third parties, such as clients, suppliers, and business contacts, should be prepared and maintained with strict accuracy and completeness. No accounts must be kept "off-book" to facilitate or conceal improper payments.

13. PROTECTION AND WHISTLEBLOWING

Employees who raise concerns or report another's wrongdoing, are sometimes worried about possible repercussions. It is the Foundation's policy that employees will not suffer retaliation or harassment for reporting in good faith any compliance concerns. The Foundation aims to encourage openness and will support anyone who raises genuine concerns in good faith under this policy, even if they turn out to be mistaken.

The Foundation is committed to ensuring no one suffers any detrimental treatment as a result of refusing to take part in financial crime, or because of reporting in good faith their suspicion that an actual or potential financial crime has taken place or may take place in the future. Detrimental treatment includes dismissal, disciplinary action, threats or other unfavourable treatment connected with raising a concern.

The Foundation ensures appropriate provisions are in place to protect employees and others who raise concerns in accordance with the Public Interest Disclosure Act 1998.

If you believe that you have suffered any such detrimental treatment, you should inform the Company Secretary immediately. If you do not feel able to raise this with the Company Secretary, this should be raised with one of the Trustees. Alternatively, the concerns should be disclosed directly to the Charity Commission.

14. QUESTIONS?

If you have any questions or concerns about anything in this policy, do not hesitate to contact the Company Secretary.

Part I: Anti-Bribery and Corruption Policy

1. INTRODUCTION

Bribery and corruption remain major issues in world trade, despite the many dedicated efforts to prevent them. They are very damaging to the societies in which they occur. These serious criminal offences:

- divert money and other resources from those who need them most;
- hinder economic and social development;
- damage business, not least by increasing the cost of goods and services.

We run our Foundation with integrity and in an honest and ethical manner. All of us must work together to ensure the Foundation remains untainted by bribery or corruption.

This policy is a crucial element of that effort. It has the full support of the Board of Trustees.

It sets out the steps all of us must take to prevent bribery and corruption and to comply with relevant legislation.

2. POLICY STATEMENT

At the Foundation, we take a strong stance against bribery and corruption. We are committed to upholding all relevant laws in every jurisdiction we operate in. We support global efforts to eliminate bribery and corruption, including the United Nations Anti-Corruption Convention and the Group of Twenty Anti-Corruption Action Plan.

As a UK registered charity, we adhere to the Bribery Act 2010 (the "Bribery Act") both domestically and internationally. We conduct thorough due diligence on our partners, grant recipients, and associates to ensure compliance with all applicable anti-bribery and anti-corruption laws.

Bribery and corruption undermine legitimate business activities and are serious criminal offences. Under the Bribery Act, individuals can face up to 10 years' imprisonment, and the Foundation could face unlimited fines, exclusion from public contracts, and reputational damage. We take our legal responsibilities very seriously.

Breaching this policy is considered a serious issue and may result in disciplinary actions, including dismissal or termination of business relationships.

3. WHAT IS BRIBERY AND CORRUPTION?

Corruption is the misuse of power for private gain, whether in public office or business. Bribery, a form of corruption, involves offering, promising, or giving anything of value to induce improper performance of a function or activity. Bribes can take many forms, including money, gifts, kickbacks, loans, fees, hospitality, services, discounts, charitable contributions, contracts, or votes.

It is also a criminal offence to bribe Foreign Public Officials to obtain or retain business or commercial advantages. The Foundation can have criminal liability for bribery committed by anyone performing services for or acting on behalf of the Foundation.

4. WHO CAN BE INVOLVED IN BRIBERY AND IN WHAT CIRCUMSTANCES?

Bribery and corruption may be committed by our:

- staff (employees, directors etc.) or anyone they authorise to do things on our behalf;
- representatives and other third parties who act on our behalf;
- suppliers; and
- customers (because they might try to induce one of our people to give them more favourable terms).

Bribery can occur in both the public and private sectors. The person receiving the bribe is usually in a position to influence the award or the progress of business, sometimes a government or other public official.

5. THE LEGAL POSITION ON BRIBERY

Bribery and corruption are criminal offences in most countries where we do business. Under the Bribery Act it is illegal for the Foundation or individuals covered by the Policy to:

- pay or offer to pay a bribe;
- receive or agree to receive a bribe; or
- bribe a foreign public official.

The Foundation may also commit an offence if it fails to prevent a person associated with it from bribing another person with the intention of obtaining or retaining business or a business advantage for the Foundation.

It does not matter whether the bribery or corruption occurs in the UK or abroad. An act of bribery or corruption committed anywhere in the world may well result in a prosecution in the UK and/or the USA, which has similar legislation. It does not matter whether the act of bribery is done directly or indirectly.

6. AREAS OF SPECIFIC RISK

We conduct a regular risk assessment to identify bribery and corruption risks facing the Foundation. We have identified certain aspects of our business where we are presented with a higher risk than others. These include:

- gifts and hospitality (see also Section 7)
- facilitation payments (see also Section 9):
  - also known as ‘grease’ payments;
  - usually small amounts paid to officials to provide goods or services to which we are already entitled, e.g., speeding up the grant of a licence or permit;
  - widespread corruption in sectors such as road transport, infrastructure, governments, especially in low and middle-income countries;
  - illegal under the Act and in many other countries where we do business;
  - we do not offer or pay them;
  - if you are faced with a request, or a demand, please report this to the Company Secretary immediately;
- activity partners, and grant recipients; and
- beneficiary relationships.

7. GIFTS AND HOSPITALITY

Our policy allows gifts, entertainment, hospitality, and promotional expenditures if they are proportionate, transparent, reasonable, and for bona fide purposes related to the Foundation's aims.

All gifts and hospitality must:

- comply with local laws;
- not be intended to influence business decisions;
- be given in the Foundation's name;
- not exceed £250 in value without prior written approval; and
- not include cash or cash equivalents.

Gifts should be appropriate, given openly, and not offered to government officials or politicians without prior approval.

In the unlikely event that a gift or hospitality with a value of more than £250 per event per person (or of comparable value in a different country) is to be given or offered (to or from a single source on a single occasion) these must have the prior written approval of the Executive Director or the Chair.

All gifts or hospitality with a value of more than £100 per event per person (or of comparable value in a different country) accepted or offered by any employee or trustee should be entered on the register of gifts.

Any approval required by the above policies relating to the Executive Director must be provided by the Chair, and vice versa.

8. WHAT IS NOT ACCEPTABLE?

It is not acceptable to:

- give or offer anything of value with the expectation or hope that this will influence decision-making or gain business advantages;
- give or offer anything of value to expedite routine procedures;
- accept or request payments or gifts with the intent or expectation of influencing the Foundation's decisions;
- retaliate against workers who refuse to commit bribery or raise concerns; or
- engage in activities that breach this policy.

9. WHAT SHOULD YOU DO IF YOU THINK SOMETHING IS WRONG?

You **must speak out** if you discover or suspect anything wrong, corrupt or otherwise improper occurring in relation to our work as a Foundation. This is essential to our maintaining integrity in what we do as a Foundation.

If you discover or suspect bribery or corruption involving:

- another staff member;
- a third party who represents us;
- one of our suppliers or competitors; or,
- anyone else in the course of your work

you **must report this immediately** to your line manager or the Company Secretary.

It is important that you raise any concerns you may have early. You may be required to explain any delays.

10. FACILITATION PAYMENTS

Facilitation payments and kickbacks are illegal. Facilitation payments are typically small, unofficial payments to government officials made to secure or expedite a routine, non-discretionary governmental action (e.g., processing a visa, customs invoice, or other governmental paper).

The Foundation does not make or accept such payments. If asked to make a payment, please report this to your line manager or the Company Secretary immediately.

11. LOCAL CUSTOMS

We understand that people in different parts of the world have different social and cultural customs. However, irrespective of where in the world we are doing business, we do not pay or accept bribes or act corruptly. This type of behaviour is expressly prohibited. However, subject to that position, we understand the need to be sensitive to local customs, e.g., there are cultures in which refusing (or failing to offer) a gift is considered impolite and could alienate a key contact or customer. In such cases, please refer to the Company Secretary.

All our people visiting regions where these cases are more common should familiarise themselves, prior to travel, with current guidance relating to those countries. For general information on travelling to a particular country, please consult the latest information from the UK government.

12. EXCEPTIONAL CIRCUMSTANCES

Payments made under extortion or duress involving imminent threats of death or serious injury may not amount to bribes. If such a payment is extorted or forced under duress then the payment may be made provided that either the Executive Director or Chair is promptly informed, the payment is appropriately recorded in Foundation's financial records as a "facilitating payment," and supporting records regarding the reason and circumstances surrounding the payment are documented in a written report.

13. RECORD KEEPING

It is essential that we keep full and accurate records of all our financial dealings. Transparency is vital in helping us demonstrate our compliance with the Bribery Act.

Maintain accurate financial records and declare all gifts and hospitality over £100. Submit expenses claims in accordance with the Foundation's policy and ensure all documents related to third-party dealings are accurate and complete.

Part II: Anti-Fraud Policy and Fraud Response Plan

1. INTRODUCTION

Fraud is a major issue affecting individuals and businesses in every country and in every sector. Fraud is incredibly damaging. It can affect the Foundation both where we:

- are the intended victim of the fraud; or
- fail to prevent an associated person committing fraud intending to benefit our Foundation.

We run our Foundation with integrity and in an honest and ethical manner. All of us must work together to ensure the Foundation remains untainted by fraud.

This policy is a central element to our anti-fraud stance and has the full support of the Board of Trustees. It sets out the steps all of us must take to prevent fraud in our organisation and to comply with relevant legislation.

2. POLICY STATEMENT

The Foundation does not tolerate fraud and will uphold all applicable laws relevant to countering fraud in all the jurisdictions in which it operates. As a UK registered charity, the Foundation remains bound by the laws of the UK, including the Fraud Act 2006, in respect of its activities both at home and abroad.

The Trustees have a legal duty and responsibility to safeguard the Foundation's money and assets, act prudently, avoid activities that may place its funds, assets, or reputation at undue risk, and take all necessary steps to ensure there is no misuse of the Foundation's funds or assets.

3. SENIOR MANAGEMENT COMMITMENT

The Board of Trustees is committed to preventing persons associated with the Foundation from committing fraud and to actively reject fraud, even if this results in short-term losses, missed opportunities, or delays. We are also committed to protecting the Foundation from falling victim to fraud.

This commitment includes:

- ensuring there is clear governance across the Foundation in respect of our fraud prevention framework;
- leading by example, including by challenging misconceptions and reducing the rationalisation of fraudulent behaviour, e.g., fraud is a "victimless crime";
- allocating reasonable and proportionate budget specifically for the leadership, staffing and implementation of our fraud risk management policy, including training, over the long term; and
- fostering an open culture within the Foundation where fraud is never acceptable and staff feel empowered to speak up early if they encounter fraudulent practices, or have any ethical concerns, no matter how minor.

4. WHAT IS FRAUD AND HOW DOES IT AFFECT US?

The Foundation can both commit and be a victim of crime in the same way as any other organisation.

Unfortunately, this risk can never be completely eliminated. Fraud may be carried out by someone connected to the Foundation, as well as a crime committed by entirely external individuals or entities. Fraud is a form of dishonesty, involving false representation, failing to disclose information, or abuse of position, undertaken in order to gain or cause loss to another. It includes acts such as deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts, and collusion.

Fraud can be committed in various ways including:

- theft – removal or misuse of funds, assets, or cash, including physical or intellectual property;
- false accounting – dishonestly destroying, defacing, concealing, or falsifying any account, record, or document required for any accounting purpose for the benefit of the Foundation or others;
- abuse of position – abusing authorities and misusing Foundation resources or information for personal gain or causing loss to the Foundation;
- misuse of equipment – deliberately misusing materials or equipment belonging to the Foundation; and
- cybercrime – including ransomware attacks, phishing scams, and spear phishing scams.

Under the Fraud Act 2006, fraud is punishable for individuals by up to 10 years' imprisonment. If the Foundation was found to have committed a criminal offence of fraud, it could face an unlimited fine, be excluded from tendering for public contracts, and face significant damage to its reputation.

The Economic Crime and Corporate Transparency Act 2023 (ECCTA 2023) introduced a corporate failure to prevent fraud that is committed for the benefit of a large organisation. Whilst the Foundation is not a large organisation and is out of scope of this offence, we do not in any way tolerate any fraud being committed for our benefit and have put in place policies and procedures to prevent this occurring.

5. FRAUD PREVENTION

Fraud is costly, both in terms of reputational risk and financial losses. It is time-consuming to identify and investigate, disruptive, and damaging. It is also a serious criminal offence. It follows that the prevention of fraud is a key objective for the Foundation. We seek to ensure that measures are in place to ensure effective leadership, auditing, and vetting procedures for trustees, employees, agents, consultants, and anyone representing the Foundation, to help deny opportunities for fraud.

Fraud can be minimised by carefully designed and consistently operated procedures. Staff are made aware of policies through the Employee Handbook and updates are circulated by email.

Our internal financial controls are designed to ensure that at all times the financial management of the Foundation is conducted in accordance with the highest standards.

Regular management review of systems and reports by internal audit in line with the agreed annual audit program should also assist in preventing and detecting fraud.

6. FRAUD WARNING SIGNS

Whilst by no means being proof alone, the circumstances below may indicate fraud, and should be treated as a warning sign:

- emails that are out of character for the sender and with instructions to make payments or disclose information;
- business emails sent from a personal email account;
- unusual discrepancies in accounting records and unexplained items on reconciliations;
- financial documents - such as invoices, credit notes, delivery notes, orders etc. – provided as photocopies rather than originals or frequently contain alterations or deletions. This might indicate counterfeit or falsified documents being used to support bogus account entries;
- high numbers of cancelled cheques, or duplicated payments or cheques;
- suppliers regularly submitting invoices electronically in non-PDF format that can be altered;
- unexplained variances from agreed budgets or forecasts;
- misdescription of purchase and expense items in the accounting system;
- inconsistent, vague or implausible responses to reasonable and legitimate queries about the accounts or accounting records, and/or queries being left unexplained, or taking a long time to resolve;
- reluctance by a volunteer, member of staff or trustee involved in handling finances to accept assistance or overprotectiveness of work;
- single member of staff or trustee have control of a financial process from start to finish with no segregation of duties;
- member of finance staff working unsociable hours or working from home without reason, and a reluctance to take holidays; or
- sudden changes to the format of financial information presented to the trustee board or senior managers which make them complicated or difficult to understand.

7. WHAT SHOULD YOU DO IF YOU THINK SOMETHING IS WRONG?

You **must speak out** if you discover or suspect any fraud occurring in relation to our work as a Foundation. This is essential to our maintaining integrity in what we do as a Foundation.

If you discover or suspect fraud by:

- another staff member;
- a third party who represents us;
- one of our suppliers or competitors; or,
- anyone else in the course of your work

you **must report this immediately** to your line manager or the Company Secretary.

It is important that you raise any concerns you may have early. You may be required to explain any delays.

8. ASSESSMENT OF RISK

We carry out regular fraud risk assessments to assess existing and emerging risks facing the Foundation. This assesses inherent risk both of the Foundation being a victim and committing fraud and the effectiveness of the controls that are in place to prevent and mitigate these risks.

We assess potential fraud risk and consider possible countermeasures whenever we introduce new products, services or arrangements with associated persons.

If you have any questions relating to emerging risks, please contact the Company Secretary.

9. SENSITIVE OR COMMERCIAL DATA

Our procedures for limiting access to sensitive and/or commercial data and identifying potentially unauthorised access are set out in our IT Security policy.

We do not permit external people to have access to our IT or security systems.

These procedures are subject to regular monitoring and review.

If you have any questions relating to data security, please contact the Company Secretary or Head of IT.

10. RECORD KEEPING

The Foundation must keep financial records for six years and have appropriate internal controls in place which will evidence the business reason for making payments to third parties.

All accounts, invoices, memoranda and other documents and records relating to dealings with third parties, such as clients, suppliers, and business contacts, should be prepared and maintained with strict accuracy and completeness. No accounts must be kept "off-book" to facilitate or conceal improper payments.

11. FRAUD RESPONSE PLAN

Total protection from fraud is not possible. In the event that the Foundation becomes involved in fraudulent activity, whether as a victim or committed for our benefit, we have procedures for responding to that fraud to manage the incident swiftly and effectively. These are set out at **Appendix B**.

Part III: Anti-Money Laundering and Terrorist Financing Policy

1. INTRODUCTION

Money laundering is a key enabler of financial crimes. We are committed to maintaining the highest standards of compliance and integrity. This policy outlines our approach to preventing and detecting money laundering and terrorist financing activities.

2. POLICY STATEMENT

The Foundation does not tolerate money laundering or terrorist financing and will uphold all applicable laws relevant to these criminal offences in all the jurisdictions in which it operates. As a UK registered charity, the Foundation remains bound by the laws of the UK, including the Proceeds of Crime Act 2002 and the Terrorism Act 2000, in respect of its activities both at home and abroad.

The Foundation is determined to prevent our being used for money laundering or terrorist financing. Through this policy we aim to deter money laundering, counter terrorist financing, and protect our resources and reputation, ensuring that we can continue to support our charitable objectives with integrity and transparency.

3. SENIOR MANAGEMENT COMMITMENT

The Board of Trustees is committed to preventing our being involved in any way with money laundering or terrorist financing.

The Foundation is committed to:

- preventing the misuse of our resources for money laundering or terrorist financing;
- complying with all applicable laws and regulations, even if not directly in scope; and
- promoting a culture of transparency and accountability within the organisation.

4. WHAT IS MONEY LAUNDERING?

Money laundering is the process by which the proceeds of crime, and the true ownership of those proceeds, are changed so that the proceeds appear to come from a legitimate source. More simply, it is the process used to disguise the true origin of money or property obtained from criminal activity. Money laundering is a criminal offence. At a basic level it involves three different stages:

- placement: this occurs when cash generated from crime is placed in the financial system. Entities or businesses which deal in cash would be particularly vulnerable to this stage of Money Laundering;
- layering: this occurs when the proceeds of criminal activity are moved around and converted into different instruments or forms in order to distances them from the illegal activity and to give them the appearance of legitimacy; and
- integration: once the origin of the criminal proceeds has been obscured, the funds are then re-entered into the legitimate economy. This may happen, for example, through investment of these 'clean' fund in a legitimate business venture.

The three basic steps may occur as separate and distinct phases, they may occur simultaneously or more commonly, they may overlap.

The techniques used by money launderers are constantly evolving to match the source and amount of funds to be laundered, and the legislative/regulatory/law enforcement environment of the market in which the money launderer wishes to operate.

There are three different criminal offences of money laundering all of which apply to employees:

- the "Concealing" offence - where a person conceals, disguises, converts or transfers property that they know or suspect is the proceeds of crime;
- the "Arranging" offence – where a person enters into or becomes involved in an arrangement that they know or suspect facilitates (by whatever means) the acquisition, retention, use or control of criminal property by, or on behalf of another person; and
- the "Acquisition" offence – where a person acquires, uses or possess property that they know, or suspect is the proceeds of crime.

If at any time you develop knowledge or suspicion of money laundering in relation to the activity of the Foundation or any person covered by this policy, you must not be involved in that activity. As set out below, you must **immediately report** that activity and seek guidance from the Company Secretary before proceeding with or continuing with that activity.

5. WHAT IS TERRORIST FINANCING?

Terrorist financing is the raising, moving, storing and using of financial resources for the purposes of terrorism. It may involve funds raised from legitimate sources, such as personal donations and profits from businesses and charitable organisations, as well as from criminal sources, such as the drug trade, smuggling of weapons and other goods, fraud, kidnapping and extortion. Terrorists use techniques like those of money launderers to evade authorities' attention and to protect the identity of their sponsors and of the ultimate beneficiaries of the funds.

The Terrorism Act 2000 criminalises terrorist financing and makes it an offence to use, possess, or raise funds for the purposes of terrorism, or enter into arrangements to provide funds or property for that purpose.

6. WHAT SHOULD YOU DO IF YOU THINK SOMETHING IS WRONG?

You **must speak out** if you discover or suspect any money laundering or terrorist financing in relation to our work as a Foundation. This is essential to our maintaining integrity in what we do as a Foundation.

If you discover or suspect money laundering or terrorist financing by:

- another staff member;
- a third party who represents us;
- one of our suppliers or competitors; or,
- anyone else in the course of your work

you **must report this immediately** to your line manager or the Company Secretary.

You must **not become involved** in any activity that you know, or suspect, involves money laundering or terrorist financing.

It is important that you raise any concerns you may have early. You may be required to explain any delays.

7. OUR KEY STEPS TO PREVENT MONEY LAUNDERING AND TERRORIST FINANCING

Risk Assessment: We will conduct regular risk assessments to identify and mitigate potential money laundering and terrorist financing risks facing the Foundation. This will identify inherent risks and assess the effectiveness of the controls we have in place to mitigate these risks.

Due Diligence: We will record and verify the identity of donors, partners, and grant recipients before commencing business activities with them. The purpose of this being to ensure they and their funds are legitimate. When verifying the claimed identity for a relationship involving a corporate entity, the ownership and control structure must be understood, and evidence obtained to prove this.

Record Keeping: We will maintain accurate records of all financial transactions and due diligence checks for a minimum of six years.

Training: We will provide regular training to our staff and volunteers to ensure they understand their responsibilities and can identify and report suspicious activities.

Reporting: All employees must make use of internal reporting arrangements to report, at the earliest opportunity, whenever they have knowledge or suspicion, of any financial crime, including money laundering. We will promptly report any suspicious activities to the relevant authorities where it is appropriate to do so.

APPENDIX B – FINANCIAL CRIME RESPONSE PLAN

Our plan and procedures for responding to fraud to manage the incident swiftly and effectively are set out below.

The purpose of this plan is to define authority levels, responsibilities for action, and reporting lines in the event of a suspected fraud.

Central to our response procedures is early detection, so prompt reporting of any concerns or suspicions is vital. We rely on you to remain vigilant and promptly report anything that does not feel right, in the correct way, as soon as possible.

All actual or suspected incidents should be reported without delay to a line manager or the Executive Director or Chair, who should as soon as possible convene a Project Group consisting of the following people or their nominees to decide on the initial response:

- the Executive Director and/or Chair who shall chair the meeting;
- the Finance Director;
- the Company Secretary; and
- others as determined by the Chair, e.g. legal or IT experts.

The Project Group will decide on the action to be taken, normally an investigation. If necessary, external specialist investigative auditors and legal experts may be appointed to support with the investigation.

The Chair of the Audit Committee should be advised at the earliest stage when an investigation under this procedure has been initiated.

1. INVESTIGATION

All allegations and reports of fraud will be investigated; the format of the investigation will be determined by the Project Group. Immediate steps should be taken to secure digital information (emails, internal messages and electronic documents) and physical assets, including computers and all potentially relevant hard copy documents.

A detailed record of the investigation should be maintained. This should include a chronological file recording details of telephone conversations, discussions, meetings and interviews, details of documents reviewed, and details of any tests and analyses undertaken. Interviews should be conducted in a fair and proper manner.

The Project Group will consider whether it is necessary to investigate systems other than that which has given rise to suspicion, through which the suspect may have had opportunities to misappropriate the Foundation's assets.

2. PREVENTION OF FURTHER LOSS

If there is thought to be any possibility of ongoing or recurring fraud, then immediate steps should be taken to prevent further losses, including suspending or recalling BACS or cheque payments.

Where there are reasonable grounds for suspecting a staff member of fraud, the staff member under suspicion will be suspended on full pay. In these circumstances, the staff member should be:

- approached without notice and asked to provide information about the allegation;
- then be suspended pending completion of the full investigation;
- supervised at all times before leaving the Foundation's premises;
- allowed to collect personal property under supervision;
- required to hand over all property in their possession belonging to the Foundation including their laptop computer, iPad, mobile phones and hard copy documents; and
- required to provide passwords for computers and mobile they have in their possession belonging to the Foundation.

The Foundation's Head of IT should be instructed to immediately withdraw access permissions to the Foundation's computer systems.

3. RECOVERY OF LOSSES

Recovery of losses is a major objective of any fraud investigation. The Project Group will ensure that, in all fraud investigations, the amount of any loss is quantified. Repayment of losses will be sought in all cases.

Where the loss is substantial, legal advice may be obtained about the need to obtain Court Orders to freeze assets belonging to the staff member(s) suspected of fraud, pending conclusion of the investigation.

Legal advice may also be obtained about prospects for recovering losses through the civil court, where the perpetrator refuses repayment. The Foundation will normally expect to recover costs in addition to losses. If appropriate, the Company Secretary will liaise with the Foundation's insurance brokers to process a claim.

4. REPORTING TO THE BOARD OF TRUSTEES

Any incident shall be reported without delay by the Chair to the Board of Trustees and updates shall be given on a regular basis on the investigation.

On completion of the investigation, a written report shall be submitted to the Board of Trustees. The report will provide, as a minimum, the following information:

- a description of the incident;
- the value of any loss or benefit to the Foundation or others impacted by the fraud;
- the people involved;
- the means of perpetrating the fraud; and
- the measures taken to prevent a recurrence; and any action needed to strengthen future responses to fraud, with a follow-up report on whether the actions have been taken. This report will represent the definitive document on which management (in a disciplinary situation) and possibly the Police (in a criminal situation) will base their decision.

The Board of Trustees will consider whether the matter should be reported to the Police and whether they should also make a report to the Charity Commission under the Serious incident reporting regime.

"Do's and Don'ts"

In addition to the procedures set out above, when a member of staff suspects that a fraud is occurring or may have occurred, they should note the following "do" and "don't" advice:

DO	DON'T
Make a prompt note of your concerns Record all relevant details, such as the nature of your concern, the names of parties you believe to be involved, details of any telephone or other conversations with names, dates and times and any witnesses. Notes do not need to be overly formal, but should be timed, signed and dated. Timeliness is most important. The longer you delay writing up, the greater the chances of recollections becoming distorted and the case being weakened.	**Be afraid of raising your concerns** The Public Interest Disclosure Act provides protection for employees who raise reasonably held concerns through the appropriate channels. You will not suffer discrimination or detriment as a result of following these procedures and the matter will be treated sensitively and confidentially where the concern raised is genuine and held in good faith.
Retain any evidence you may have The quality of evidence is crucial and the more direct and tangible the evidence, the better the chances of an effective investigation.	**Investigate the Matter Yourself** There are special rules relating to the gathering of evidence for use in criminal cases. Any attempt to gather evidence by persons who are unfamiliar with these rules may undermine the case.
Report your suspicions promptly All concerns must be reported to a line manager, the Executive Director or the Chair.	**Discuss the matter with anyone other than your line manager, Executive Director or Chair** There may be a perfectly reasonable explanation for the events that give rise to your suspicion. Spreading unsubstantiated concerns may harm innocent persons.