# ANTI FRAUD POLICY AND FRAUD RESPONSE PLAN

## 1. POLICY STATEMENT

1.1 The FIA Foundation (Foundation) takes a zero-tolerance approach to fraud and will uphold all applicable laws relevant to countering fraud in all the jurisdictions in which it operates. It welcomes the international community's efforts to stamp out fraud. As a UK registered charity (charity no. 1088670) the Foundation remains bound by the laws of the UK, including the Fraud Act 2006 and the Bribery Act 2010, in respect of its activities both at home and abroad.

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

1.2 The purpose of this policy is to:

- set out the Foundation's responsibilities in observing and upholding its policy on fraud;
- provide information and guidance to Foundation employees and partners, grant recipients and their associates on how to recognise and deal with fraud issues; and
- establish standards of conduct for Foundation employees and partners, grant recipients and their associates so as to ensure that the relevant legislation is not violated.

1.3 This policy and the Fraud Response Plan form part of a series of related Foundation policies and procedures developed to provide sound internal financial controls and to counter any fraudulent activity. These include: codes of conduct for staff and trustees; anti-corruption and bribery policy; sanctions policy; safeguarding policy; privacy policies; sound internal control systems; effective internal audit; effective recruitment and selection procedures; disciplinary procedure; public interest disclosure (whistleblowing) procedures; register of interests for trustees; and training.

1.4 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.

## 2. WHO IS COVERED BY THE POLICY?

2.1 This policy applies directly to Foundation trustees and to all individuals working within the Foundation as employees, agents, consultants or other persons who may represent the Foundation from time to time. The policy is provided to other Foundation partners, grant recipients and associates, who will be required to take reasonable steps to ensure that, in carrying out activities supported by the Foundation, they and their directors, officers, employees and associates comply with all applicable anti-fraud laws.

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

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

## 3. WHAT IS FRAUD?

3.1 Charities can be victims of crime in the same way as any other organisation and 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.

3.2 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.

3.3 The term is used to describe such acts 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 the following:

- 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, with a view to personal gain or gain for another, or with the intent to cause loss to the Foundation or furnishing information, which is or may be misleading, false or deceptive;
- 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;
- Cybercrime – an "umbrella" term for lots of different types of crimes which either take place online or where technology is a means and/or target for the attack, including:
  i) ransomware attacks – a type of malicious software ("malware") designed to block access to a computer system until a sum of money is paid;
  ii) "phishing" scams – emails sent by fraudsters seeking to obtain sensitive information such as passwords, usernames, bank details or other financial information by electronic means (including emails, pop ups or fake websites) from seemingly trustworthy sources; and
  iii) "spear phishing" scams – emails sent by fraudsters which appear to have been sent by a senior person within an organization instructing an employee to transfer funds or provide sensitive information.

Under the Fraud Act 2006, fraud is punishable for individuals by up to 10 years' imprisonment and if the Foundation was found to have committed an offence, it could face an unlimited fine, be excluded from tendering for public contracts, and face damage to its reputation. It therefore takes its legal responsibilities very seriously.

## 4. PREVENTION

4.1 Fraud is costly, both in terms of reputational risk and financial losses, as well as time-consuming to identify and investigate, disruptive and unpleasant. The prevention of fraud is therefore a key objective. Measures should be put in place to deny opportunity and provide effective leadership, auditing, employee screening procedures, which deny opportunities for fraud.

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

4.3 The internal financial controls help 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 programme should assist in preventing and detecting fraud; and should also result in continuous improvements. The risk of fraud should be a factor for consideration in audit plans.

The credibility and success of the Anti-Fraud Policy and Fraud Response Plan is dependent largely on how effectively it is communicated throughout the organisation. To this end, details of the Policy and Fraud Response Plan will be provided to all staff and trustees.

## 5. YOUR RESPONSIBILITIES

5.1 You must ensure that you read, understand and comply with this policy.

5.2 The prevention, detection and reporting of fraud are the responsibility of all those working for the Foundation or under its control. You are required to avoid any activity that might lead to, or suggest, a breach of this policy.

5.3 You must notify your line manager as soon as possible if you believe or suspect that a conflict with this policy or the Fraud Act by an employee or third party has occurred or may occur in the future.

5.4 Any employee who breaches this policy will face disciplinary action, which could result in dismissal for gross misconduct. The Foundation also reserves the right to terminate its contractual relationship with its partners, grant recipients, and associates if they breach this policy.

## 6. RECORD-KEEPING

6.1 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.

6.2 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.

6.3 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.

## 7. HOW TO RAISE A CONCERN

You are encouraged to raise concerns about any issue or suspicion of malpractice at the earliest possible stage. If you are unsure whether a particular act constitutes fraud, or if you have any other queries, these should be raised with the Director of Governance and Personnel. Concerns should be reported as a protected disclosure to your line manager or a Director. Statutory protection of whistle blowers is afforded under the Public Interest Disclosure Act 1998.

## 8. PROTECTION

8.1 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.

8.2 The Foundation is committed to ensuring no one suffers any detrimental treatment as a result of refusing to take part in fraud, or because of reporting in good faith their suspicion that an actual or potential fraudulent act 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. If you believe that you have suffered any such treatment, you should inform the Director of Governance and Personnel immediately.

## 9. TRAINING AND COMMUNICATION

9.1 All Foundation employees will receive relevant training on how to adhere to this policy.

9.2 The Foundation's zero-tolerance approach to fraud will be communicated to all partners, grant recipients, associates, suppliers, and contractors at the outset of its relationship with them and as appropriate thereafter.

## 10. WHO IS RESPONSIBLE FOR THE POLICY?

10.1 The Board of Trustees has overall responsibility for ensuring this policy complies with the Foundation's legal and ethical obligations, and that all those under our control comply with it.

10.2 The Director of Partnerships, for programmes questions, and the Director of Governance and Personnel, for all other questions, have primary and day-to-day responsibility for implementing this policy and for 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 made aware of and understand this policy and are given adequate and regular training on it.

## 11. RISK ASSESSMENT, MONITORING, AND REVIEW

11.1 As part of its annual risk assessment process the Board of Trustees will monitor the effectiveness and review the implementation of this policy, considering its suitability, adequacy and effectiveness. The Director of Governance and Personnel will carry out regular audits of the Foundation's control systems and procedures to provide assurance that they are effective in countering fraud.

11.2 All employees are responsible for the success of this policy and should ensure they use it to disclose any suspected danger or wrongdoing.

11.3 This policy does not form part of any employee's contract of employment and it may be amended at any time.

## FRAUD RESPONSE PLAN

The purpose of this plan is to define authority levels, responsibilities for action, and reporting lines in the event of a suspected fraud. This plan may not be appropriate for concerns that are not fraud related such as bribery, anti-competitive behaviour or other irregularity.

1. 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 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;
   - Director of Governance and Personnel; 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 carry out the investigation.

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

**INVESTIGATION**

3. 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 physical assets, including computers and any records thereon, and all other potentially evidential documents.

4. 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.

5. 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.

**PREVENTION OF FURTHER LOSS**

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

7. 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 suspect(s) should be approached unannounced and should be interviewed about the allegation prior to being informed of their suspension. They should be supervised at all times before leaving the Foundation's premises. They should be allowed to collect personal property under supervision but should not be able to remove any property belonging to the Foundation.

Any security passes and keys to premises, offices, and furniture should be returned. Laptop computers, mobile phones, iPad etc. and associated hardware/software must also be returned. The Foundation's Head of IT should be instructed to immediately withdraw access permissions to the Foundation's computer systems.

**RECOVERY OF LOSSES**

8. 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.

9. Where the loss is substantial, legal advice may be obtained about the need to freeze the suspect's assets through the court, pending conclusion of the investigation.

10. 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 Director of Governance and Personnel will liaise with the Foundation's insurance brokers to process a claim.

**REPORTING TO THE BOARD OF TRUSTEES**

11. 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.

12. On completion of the investigation, a written report shall be submitted to the Board of Trustees containing a description of the incident, including the value of any loss; the people involved; the means of perpetrating the fraud; 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.

13. 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.

**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 over-protectiveness 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.

## "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 take notice of the following "do" and "don't" advice:

| DO | DON'T |
|---|---|
| **Make a prompt note of your concerns**<br>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.<br><br>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**<br>The Public Interest Disclosure Act provides protection for employees who raise reasonably held concerns through the appropriate channels.<br><br>You will not suffer discrimination or victimisation 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**<br>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**<br>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**<br>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**<br>There may be a perfectly reasonable explanation for the events that give rise to your suspicion. Spreading unsubstantiated concerns may harm innocent persons. |

**Adopted by the Board of Trustees 26 March 2013,**
**Updated and approved 17 October 2018**
**Updated and approved 13 October 2021**