FRAUD MITIGATION POLICY

Policy Summary

The purpose of this policy is to outline Esmée Fairbairn Foundation's stance on fraud, bribery and corruption and its approach to preventing, detecting, reporting and investigating fraud, bribery and corruption.

Fraud is defined in this policy as an act carried out either by any internal or external source with the deliberate intention of deceiving the Foundation, its beneficiaries, grantees or the general public to gain a personal advantage, or cause loss to another. This includes offers to pay bribes, solicitation of bribes and demands to make facilitation payments.

Esmée Fairbairn Foundation has a zero-tolerance approach to fraud and corruption, of any type or in any circumstances, whether perpetrated by Trustees, employees, volunteers, contractors, partners, grantees or other; and is determined to prevent, and where this is not possible, to detect and investigate such acts.

1 Preventing and Detecting Fraud and Corruption

The Foundation does not accept any level of fraud, bribery or corruption within its grantee organisations, partners or contracted service providers, or by any other individual or organisation receiving funds from or representing the Foundation.

The Foundation will seek to take disciplinary or other appropriate legal action against those found to have perpetrated, be involved in, or assisted with fraudulent or other improper activities in any of its operations.

The Foundation expects all those receiving funds or representing Esmée Fairbairn, including its grantees, partners, contractors, associates and service providers to have the highest standards of honesty at all times and requires all those receiving funds or representing the Foundation, to act in accordance with this.

The Foundation will work with relevant stakeholders, including comparable organisations, relevant regulators and government organisations to tackle fraud and is committed to developing an anti-fraud culture and keeping the opportunities for fraud, bribery and corruption to an absolute minimum.

2 Deterrence and Detection

The Senior Management Team are responsible for reducing opportunities for fraud and corruption and improving detection rates, supported by guidance from the Board of Trustees.

The Foundation will seek to continually assess the nature and extent of its exposure to the risks of internal and external fraud, bribery and corruption through regular monitoring and audit processes.

The Chief Operating Officer will lead the process and all staff share some responsibility in ensuring due diligence in this process by identifying the risks to which our assets are exposed, developing adequate controls across departments, and ensuring effective compliance.

The Foundation currently has the following procedures in place.

3 Reporting

3.1 Internal; Staff Reporting Procedures

All staff are responsible for reporting suspicions of fraud through the correct channels, knowing they are protected under the Whistleblowing Policy.

All staff must report any suspected or actual instances of fraud, bribery or corruption immediately to their line manager and/ or to the Chief Operating Officer, or the Chief Executive if the Chief Operating Officer is not available.

All allegations brought to the Foundation's attention should be brought to the attention of the Chief Operating Officer, who will decide whether the Chair of the Audit & Risk Committee, or Chair of the Board of Trustees, along with any relevant authorities, need to be informed.

All major incidents are escalated to the Chair of ARC and Chair of the Board of Trustees for review and decision. The COO will advise if this meets the threshold for the Foundation to submit a Serious Incident Report (SIR) to the Charity Commission.

3.2 Internal: Applications and Grants procedures

Executive staff conduct continual and thorough cross-checks of grantee account and governance documentation for all applications and organisations prior to the approval and releasing of funds.

The Foundation requires all applicants to have a constitution, or governing documents and all registered charities are checked against the Charity Commission website. If an applicant is not a registered charity, we request to see a copy of the applicant organisation's constitution and require the work we are being requested to fund to fall within the legal definition of what is charitable (this is a term of all grants made).

The Foundation performs an assessment of the applicant's governance and produces guidance (which have been confirmed by the Trustee Board) to support staff with this.

All organisations must provide financial accounts (generally which will have been either independently examined or audited) and each application must be signed off / confirmed by their Chair or equivalent senior management member.

The Foundation will have spoken to every organisation it funds, and will have reviewed organisational documents: accounts, constitution (where relevant), management accounts and a strategic plan by the time of grant recommendation.

When an organisation receives a grant offer from the Foundation, they must confirm their agreement to the Foundation's core terms and conditions, and upload evidence of their bank (either a copy of a statement received in the post, a paying in slip, a cheque copy or a signed bank letter) before any payment can be approved. See the Finance section for further detail.

During the application process staff partake in peer review of applications and provide a second pair of eyes for applications moving towards approval.

EF Trustees and staff complete a Declaration of Interest annually. Staff will not assess applications from organisations where they have an interest. Trustees and staff exclude themselves from decision-making where they have a related party interest. Conflicts of interest is a standard item on all decision-making agendas and these are minuted.

3.3 External Grantee Procedures

Trustees, employees, volunteers, grantees, partners, contractors, associates, service providers and the public are encouraged to report any suspicions or significant events relating to fraudulent or suspected fraudulent activities by phone or in writing to the Foundation as soon as they are made aware.

Grantees are required to report all major incidents of actual or potential Fraud to the Foundation in accordance with their terms and conditions. The terms and conditions request that Grantees inform the Foundation if a Serious Incident Report is made (all grant receiving Charitable organisations are duty-bound to inform the Charity Commission via a 'Serious Incident Report') and asks non-charities to inform the Foundation if there has been a serious incident.

Consultants, contractors, service providers who have access to the Foundations internal systems are regulated by the Data Protection systems in place as part of the Foundations IT coverage. All systems access is granted through a signed contract which clearly details the names of those holding responsibility for each action.

4 Governance

4.1 Risk and internal control systems

The Foundation regularly reviews and evaluates the effectiveness of its systems, procedures and internal controls for managing the risk and fraud risk management, assurance processes and audit arrangements through bi-annual reports to the Audit & Risk Committee and six annual Board Meetings with Trustees.

The Foundation's Authority Levels Policy outlines who can approve commitments and who can approve execution (including documents and payments). The policy covers grant funding, social investments, operations, and investment activity. This is reviewed by FAC and approved by the full Board annually.

The Foundation reviews these risks annually, using information on actual or suspected instances of fraud, bribery and corruption to inform its review, put in place efficient and effective systems, procedures and internal controls to prevent and detect fraud, bribery and corruption; and reduce the risks to an acceptable level.

All documentation of the Foundation systems and controls are subject to 'critical review' by senior staff members to identify, and raise the subject of, potential residual risks throughout each process.

The central list of reported fraud sits with the Chief Operating Officer.

The risk register is reviewed quarterly at the Senior Management Team Meeting, bi-annually at the Audit & Risk Committee, and annually at the December Board of Trustee Meeting.

4.2 IT & Data

The Foundation employs Ramsac as its primary IT infrastructure supplier. It is responsible for, amongst other things: the maintenance and upkeep of the boundary firewalls for the Foundation's

network, and the encryption, anti-virus, and anti-malware protection of the internal staff workstations.

Ramsac produce monthly IT Reports for the Foundation (sent to the Technology Lead and COO), which include information on the health of the network and its workstations, along with any areas of concern.

Ramsac also alerts the Foundation of any suspicious activity; including but not limited to logins to staff accounts at unusual times or from unusual geographic locations.

Ramsac are an ISO 9001 and Cyber Essentials accredited organisation.

Access to most Foundation systems is provided via Single Sign On (SSO), which is linked to the individuals Microsoft Azure account.

Where SSO is not possible, accounts are protected with passwords that follow a robust policy. Access to the data held in these systems is not possible without a Foundation login, or at the express authorisation of a staff member. Examples of this include access to the Salesforce environment for Lightful, or selected documents from SharePoint being shared with external members for the purpose of collaboration. All cases of sharing access with externals is auditable and can be revoked at any time.

Actions across Salesforce and Microsoft SharePoint – the two primary repositories for data within the Foundation – are auditable by the external IT function provided by Ramsac, at the request of a member of the senior management team.

The finance system – Sage – is managed and reviewed by the Head the Finance. (Permissions are granted by log in credentials).

Data across the Foundation's estate is protected in several ways:

- Workstations are encrypted with AES 256-bit keys, protecting any data locally stored on the devices in the event of loss or theft of the device.
- Access to the workstations is provided via Microsoft Azure, with staff accounts protected with passwords which must abide by a robust password policy.
- Data stored in the Foundation's Microsoft SharePoint instance can only be accessed via an internal staff account, or at the direct invitation of one. Access to files and folders on the SharePoint instance is monitored regularly for suspicious activity.
- Salesforce is the Foundation's Customer Relationship Management platform, which stores data of organisations and individuals who are stakeholders– either because they are in receipt of grant funding, are currently requesting grant funding, or otherwise.
- Financial data is processed by Business One Financials. Only members of the Foundation's finance team, and relevant members of senior management, have access to the platform. The platform draws information from Salesforce but exists as a separate entity.

4.3 Finance

i) Grantee and social investment payments

We have a distinction in roles within Salesforce between those recommending grants and those authorising them. Additionally, payments are entered into the banking system by one staff member, checked by another and approved in the system by a third (according to the delegation of authority). No one staff member can approve all stages through to final payment.

A funding manager can only bring forward a grant payment by three months. If the payment is brought forward by more than this, then the Chief Operating Officer is needed in order to make the change in Salesforce. If a current grant is due to be assigned to a new organisation, it must be discussed with the relevant Impact Director, following the standard procedure, in order to secure approval and permission.

The submission of bank details and a supporting document (copy of a statement received in the post, a paying in slip, a cheque copy or a signed bank letter) is a requirement on Salesforce for all grant requests. In order for the requirement to be completed it must be reviewed by two Finance or Resources staff members (usually done by the Finance Assistant, Finance Officer or Head of Finance). The first payment on a grant request cannot be moved forward to the ready-to-pay queue until both checks are complete.

If there is any change to the grantee bank details during the lifetime of the grant, we request the same information (i.e. submission of bank details and supporting document via Salesforce) via an email to two addresses in the organisation, we also confirm the change by telephone. The Head of Finance reviews a list of all organisations on a weekly basis whose bank details have been changed to ensure this match with expectations.

We have a minuted, auditable trail of all funding decisions and approvals that are made. The minutes note who the authorising signatory is as per our Approvals Levels Policy, and who else attended the Panel/Meeting in relation to required quorum for approvals.

ii) Operational cost payments

All invoices are checked by the member of staff with the most knowledge of the item and approved by a second staff member in accordance with the Authority Level Policy (generally a member of the SMT). Operational cost payments are entered into the banking system by one staff member, checked by another and approved in the system by a third (according to Authority Level Policy).

iii) Additional Internal Controls

- Management Accounts and supporting analyses including budgeted versus actual costs are prepared monthly and circulated to the SMT by the Head of Finance. Latest available Management Accounts are also included with Board Papers.
- The Chief Operating Officer and Head of Finance submit/input the payroll together once a month via the payroll provider's portal. The Finance Officer will support this process in the absence of either the COO or HoF. The resulting reports are reviewed by both the Chief Operating Officer and Head of Finance before pay slips are distributed to staff. The payroll journal entry is uploaded by the Finance Assistant/Finance Officer and reviewed and posted by the Head of Finance.
- Bank reconciliations are prepared monthly by the Finance Assistant/Finance Officer and reviewed/approved by the Head of Finance.
- All balance sheet items are reconciled quarterly by the Finance Assistant/Finance Officer, these working papers are reviewed and approved by the Head of Finance.
- As the majority of journal entries are processed by the Finance Assistant a monthly list of journal entries is created from the finance system by the Head of Finance who reviews it and then passes to the Chief Operating Officer for review.

- Phishing emails received are passed on to the Technology Lead to block the sender's accounts.
- Social Investment bad debt or provisions for bad debt are approved by the Chief Executive and reported as part of the management accounts.
- Our external auditors conduct fieldwork for the annual audit in c. October and March each year, although fraud detection is not within the scope of their engagement, they report any fraud they come across.

4.4 Investment

The Foundation uses the following controls to mitigate the risk of falling foul of fraud/bribery:

- All of the Foundation's investment recommendations have been through separate due diligence performed by our investment advisor (Cambridge Associates).
- The Foundation obtains an external legal opinion before proceeding with any new investment – this includes a review of the structure of the investment vehicle and whether anything is outside market practice.
- A number of the Foundation's core holdings are in "regulated" investment vehicles – these are industry-standard funds where the risk of fraud should, in theory, be lower. (Incidents of fraud in investment funds are often higher in "unregulated" funds.)
- For larger investment payments the Foundation requires more than one approver – both in terms of permission for a payment to go ahead and on execution of a deal. This is outlined in the Authority Levels Policy.
- Finance and Investment staff have access to JPM's online system. User's roles are managed to ensure inputter/approver duties and approval limits are in line with the delegation of authority. Cash movements for trades instructed by Esmée are handled by JPM. Investment cost invoices, after being checked and approved in line with the delegation of authority are emailed to JPM who handle the payment, JPM perform a call back function for any new vendors. Fund accounting and portfolio valuation is performed monthly by JPM, the resulting reports are checked by Esmée staff.
- A lesser, but related, point is that the Foundation's policy is for staff to not accept any corporate hospitality or gifts of any kind from investment managers. Where this occurs e.g. through gifts of chocolates or wine at Christmas or similar occasions, they are placed in a staff raffle.

5 Related Policies and Procedures

i) Internal

- Esmée Fairbairn Foundation – Fraud and Bribery Policy
- Esmée Fairbairn Foundation – Data Protection Policy
- Esmée Fairbairn Foundation – Authority Levels Policy

ii) External

- The Fraud Act 2006. Relevant legislation in the UK
- ACF guidance to help members deter and detect external grant fraud
- The Charity Commission Fraud Strategy Information to support charities against fraud.

Approved: Audit and Risk Committee 10 June 2025