FRAUD MITIGATION AND BRIBERY POLICY

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.

Oversight of the Foundation's approach to Fraud and Bribery is delegated to the Audit and Risk Committee, reporting to the Board of Trustees.

What is Fraud?

Fraud is defined in this policy as an act carried out either by an internal source (staff, trustee, volunteer) 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. It covers acts varying from theft to false accounting and bribery, from a supplier who dishonestly invoices for work that they haven't done, to the candidate who falsely claims qualifications on their CV. It may involve not telling the truth, failing to say something when you should, or abusing your position.

The Foundation's attitude to fraud

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

The Foundation expects that its trustees, staff and volunteers will always have the highest standard of honesty. The Foundation expects all those receiving funds or representing Esmée Fairbairn, including its grantees/fundees, 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.

1 Preventing and detecting fraud and corruption

Fraud prevention and detection is the responsibility of everybody in the Foundation. All can be aware of the risk of fraud and suggest processes for preventing and detecting many frauds.

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. Any staff or trustees who do not comply with this policy may be subject to disciplinary procedures.

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 Promoting an anti-fraud and anti-corruption culture

The Foundation aims to attract Trustees, employees and others who have a positive attitude to protecting and making best use of its assets as well as achieving its objectives.

The anti-fraud and bribery policy is supported by other policies including the Whistleblowing Policy, the Conflict-of-Interest Policy and ICT policy.

3 Deterrence and detection

Although Trustees are ultimately responsible for reducing opportunities for fraud and corruption and improving detection rates, the COO alongside the SMT will advise and lead on the process. All staff are responsible for reporting suspicions of fraud through the correct channels, knowing they are protected under the Whistleblowing Policy.

Major deterrents to perpetrating fraud and corruption are the risk of being caught and the severity of the consequences. The Foundation will take robust action, including prosecution, against those who commit fraud. In addition to reporting the fraud to the Police, the Foundation will actively pursue the recovery of monies, using legal means, when appropriate.

4 Reporting

It is the responsibility of all staff to report suspected, actual or attempted fraud or corruption. The provisions of the Whistleblowing Policy can be followed in such circumstances.

All reported instances of actual, attempted or suspected fraud or corruption will be investigated and appropriate action taken against the perpetrator. Control weaknesses identified as a result of reported instances will be addressed with immediate effect to prevent future similar occurrences.

Fraud Mitigation Procedures

The following outlines Esmée's response and actions to fraud and provides guidance for staff and trustees to prevent and respond to instances of fraud.:

5 Oversight and controls

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 Chief Operating Officer (COO) will lead the process, and all staff share 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 documentation of systems and controls, not just in Finance but throughout the Foundation's activities is important. It is not just about having those systems and controls written down, they need to be subject to 'critical review' by all staff members to identify, and raise the subject of, potential residual risks.

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.

6 Reporting

6.1 Internal - Staff Reporting Procedures

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

The Chief Operating Officer will maintain a register of all frauds and corrupt practices, actual and attempted, and report on these matters, including actions taken, to the Audit & Risk Committee.

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 or Action Fraud/the Police.

There is a requirement to report major instances of fraud or corruption to the Charity Commission as soon as these come to light (through a Serious Incident Report) and on an annual basis as part of the Charity Commission Annual Return. The Charity Commission must also be informed of any reporting to the Police. The Chief Operating Officer is responsible for making these disclosures and completing the annual return to the Commission.

6.2 Internal - Applications and Grants procedures

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

The Foundation requires applicants to have a constitution, or governing documents and 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 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 details (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.

The Foundation's 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.

6.3 External Grantee Procedures

Trustees, staff, 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, and 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.

7 Governance

7.1 Risk and internal control systems

The Foundation regularly reviews and assesses how effective its systems, procedures, internal controls, fraud risk management, assurance processes, and audit arrangements are. This oversight is supported through reports to the Audit & Risk Committee and Board as appropriate.

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 Finance and Administration Committee (FAC) and approved by the Board annually.

The Trustees review risk approach regularly, 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. This is led by the Audit and Risk Committee.

All documentation of the Foundation's 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 COO.

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.

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

Ramsac provide a live dashboard for the Foundation (accessible by the Technology Lead and COO), which includes 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, ISO 27001 and Cyber Essentials Plus accredited organisation.

Access to most Foundation systems is provided via Single Sign On (SSO), which is linked to the individual staff member's 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 or selected documents from SharePoint being shared with external members for the purpose of collaboration. All cases of sharing access with external parties are 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 – Microsoft Dynamics 365 Business Central (BC) – is managed and reviewed by the Head of Finance. (Permissions are granted by log in credentials - the Head of Finance can purchase new licenses, but the Technology Lead must assign licenses to users.)

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 BC. 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.

7.3 Finance

i) Grant 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 COO is needed in order to make the change in Salesforce, and the rationale for this is documented. 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, and documented in Salesforce.

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. With more grantees being digital only and not able to supply a scan of a paper document the Finance team use the Confirmation of Payee (CoP) checks within RBS Bankline and/or call grantees on a phone number known to be correct to verify bank details provided. In order for the requirement to be completed it must be reviewed by two Finance or Resources

staff members. 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 the organisation using an address known to be correct, we also confirm the change by telephone. The Head of Finance reviews a list of all organisations on an ongoing basis whose bank details have been changed to ensure this matches with expectations, this is done via the Task function on the home screen of Salesforce.

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. Invoices are entered into BC by the Finance Assistant / Finance Officer and checked and posted by the Head of Finance. These functions can only be performed by staff members with access to BC. Operational cost payments are entered into the banking system by one staff member, checked by another and approved in the system by a third in line with the Authority Levels Policy. Entry and approval can only be performed by staff members with access to RBS Bankline. RBS Bankline requires dual approval for changes such as adding new users or adding new countries where payments can be made to.

iii) Additional Internal Controls

- Management Accounts and supporting analyses including budgeted and forecasted versus actual costs are prepared monthly and circulated to the COO, Chief Executive and Director of Social and Impact Investment by the Head of Finance. SMT reviews grant budget and grant spend information at each meeting. Latest available Management Accounts are also included with each set of Board Papers.
- The Chief Operating Officer, Head of Finance and Finance Officer submit/input the payroll once a month via the payroll provider's portal. 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 at least quarterly by the Finance Assistant/Finance Officer, these working papers are reviewed and approved by the Head of Finance.
- All journal entries require an inputter and an approver (fixed asset disposals and depreciation being the exception). The approval workflow within BC ensures that payment journals are sent to an approval group made up of the Finance Officer, Head of Finance, COO, Director of Social and Impact Investment, and Chief Executive. If the Finance Officer submits a payment journal for approval the entry is sent to an approval group with the same members as above apart from the Finance Officer. If the Head of Finance submits a payment journal for approval the entry is sent to an approval group with the same members as above apart from the Finance

Officer and Head of Finance. All non-payment journal entries are sent for approval to a user group made up of Head of Finance, COO, Director of Social and Impact Investment, and Chief Executive unless the entry is submitted for approval by the Head of Finance in which case the entry is sent to an approval group with the same members as above apart from the Head of Finance. The Finance Assistant or Head of Finance run an all journal entries report twice a year, the Head of Finance reviews the report for any unusual items. This report is also provided to the auditors.

- 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 would report any fraud they came across.

7.4 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/s.
- 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 are in line with the delegation of authority. Cash movements for trades instructed by the Foundation 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. Other cash movements such as the payment of the Operational Transfer from JPM to the RBS operating account or the payment of margin calls for the Foundation's currency hedging programme are approved by email, entered on the JP Morgan system (JP Morgan Markets or JPMM) by one staff member and approved/checked by another. Capital calls from the Foundation's private equity investments are entered (and checked) on the JPM system by JP Morgan and then approved by two members of staff from the two different JPMM user groups. Capital calls over £250k are approved by email in line with the Authority Level Policy. Fund accounting and portfolio valuation is performed monthly by JPM, the resulting reports are checked by Foundation staff.
- 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 minor food gifts at Christmas or similar occasions, they are placed in a staff raffle or shared with all staff.

8 Related Policies and Procedures

i) Internal

- Esmée Fairbairn Foundation – Authority Levels Policy
- Esmée Fairbairn Foundation – Conflict of Interest Policy
- Esmée Fairbairn Foundation – Data Protection Policy
- Esmée Fairbairn Foundation – Whistleblowing Policy

ii) External

- The Fraud Act 2006. Relevant legislation in the UK
- The Bribery Act 2010. Relevant legislation in the UK
- ACF Guidance to help members deter and detect grant fraud
- The Charity Commission Fraud Strategy Information to support charities against fraud.

Approved: Audit and Risk Committee, 03 November 2026