Anti-Fraud, Anti-Bribery and Corruption Policy

Synopsis

This policy outlines the NSPCC's attitude and approach to fraud with guidance on the associated procedures relating to our fraud risk management.

Failure to follow the procedures set out in this policy may result in disciplinary action.

Applicable

This policy is applicable to all employees, agency staff, contractors, volunteers, trustees and donors.

Effective Date: October 2022

Author: Allison Howe

Last Review Date: March 2024

Next Review Date: March 2027

1. Fraud Policy Statement - why the policy is important

Introduction

1.1. Policy Statement

The NSPCC has a policy of zero tolerance of fraud, bribery and corruption.

The purpose of the policy statement is to ensure that we continue to have high standards and clear guidance on the NSPCC's organisational approach to addressing the risks of fraud, bribery and corruption and sets out our responsibilities for its prevention. This policy also refers to the Anti-Fraud, Anti-Bribery and Corruption Response Plan (the 'Fraud Response Plan' attached at Appendix A), which outlines the action to be taken if you discover or suspect fraud.

1.2. The NSPCC requires all employees and related Third Parties to act in an honest and ethical manner with integrity and to safeguard the resources for which they are responsible. Fraud is an ever-present threat to these resources and hence must be of concern to all employees and anyone associated with or acting on behalf of the NSPCC. It is unacceptable for anyone associated with the NSPCC to take part in acts of fraud.

1.3. The NSPCC will uphold all laws relevant to countering fraud, bribery, and corruption including money laundering in all jurisdictions it operates in and expects its employees and related Third Parties to abide by these laws.

What is Fraud?

1.4 The term **fraud** is used to describe a whole range of activities such as: deception; **bribery**; forgery; extortion; **corruption;** theft; conspiracy; embezzlement; misappropriation; false representation/accounting, concealment of material facts and collusion and **money laundering**.

Generally, however, fraud involves the intention to deceive a person or organisation in order to obtain a financial advantage, or personal gain, or to cause a loss to another party.

The term fraud also includes the use of information technology equipment to manipulate programmes or data dishonestly.

1.5 **Bribery** involves an inducement or reward offered, promised, provided or received in order to gain or give any commercial, contractual regulatory or personal advantage.

1.6 **Corruption** is the misuse of entrusted power for personal gain. This would include dishonest or fraudulent behavior by those in positions of power, such as managers or government officials. It would include offering, giving and receiving bribes to influence the actions of someone in a position of power or influence, and the diversion of funds for private gain.

1.7 **Money Laundering** is attempts to make illegally obtained money appear legitimate. For a charity, this is often carried out when bogus 'donations' are given and then the 'donor' asks for them to be refunded.

1.8 **Third Parties** includes agency staff, contractors, volunteers, trustees, donors, and other 'related' third parties would include individuals/groups who are not employees, and organisations with whom there is some connection with the NSPCC eg through a fundraising event.

What the policy involves

1.9 **The NSPCC's Attitude to Fraud** – the NSPCC takes the most serious view of any attempt to commit fraud by employees, agency staff, suppliers, contractors including their employees and agents acting on behalf of the NSPCC, volunteers, trustees, donors and others.

1.10 **Fraud, Bribery and Money Laundering** are criminal offences and qualify as acts of gross misconduct.

2. How to comply

2.1 **NSPCC's responsibilities:**

- The NSPCC is responsible to the Board of Trustees who are required under charity law to safeguard the assets of the charity.
- The Finance, Audit & Risk Committee is responsible for approving any changes to this policy.
- The Head of Governance, Risk and Compliance has primary responsibility for implementing this policy, providing assurance of compliance and assistance to answer any queries arising from its interpretation.
- The Head of Governance, Risk and Compliance is responsible for monitoring the effectiveness of this policy. Annual Assurance Statements completed by Executive Board Directors and submitted to Finance, Audit & Risk Committee/Board of Trustees includes Anti-Fraud, Anti-Bribery and Corruption risk assessment -see attached Appendix B.

2.2 **Risk and internal control systems**

The NSPCC will:

- seek to assess the nature and extent of its exposure to the risks of internal and external fraud, bribery and corruption. It will regularly review 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: encourage an anti-fraud culture; prevent and detect fraud, bribery and corruption; and reduce the risks to an acceptable level;

- in order that employees have the skills, knowledge and expertise to manage its fraud risk effectively, it will provide induction and refresher training to help make employees aware of the risks of fraud, bribery and corruption, and of their responsibilities in preventing, detecting, and reporting it;

- make all those receiving NSPCC funds or representing the NSPCC, including its employees, agency staff, contractors, volunteers, donors, trustees and suppliers aware of this policy;

- provide information to relevant stakeholders, for example via procurement/contractual processes, the intranet, regulatory requirements, including comparable organisations, relevant regulators and government organisations to tackle fraud.

- regularly review and evaluate the effectiveness of its systems, procedures and internal controls for managing the risk of fraud. It will do this through risk management and assurance processes and audit arrangements.

2.3 Employee Responsibilities

2.3.1 **Line managers** are responsible for:

the prevention and detection of fraud by undertaking training at induction and refresher training aiming to ensure that an adequate system of internal controls exists within their areas of responsibility, and these controls operate effectively. This is to aim to ensure that all their employees and volunteers are aware, trained, understand and comply with this policy and support the Head of Governance, Risk and Compliance in providing Trustees with the assurance that the policy is being complied with and complying with any regulatory requirements including Reporting Serious Incidents to the Charity Commission.

2.3.2 **Every employee,** agency staff, contractors, volunteers, trustees, donors, and other Third Parties associated with the NSPCC have a responsibility to:

ensure that public funds, the NSPCC's reputation and its assets are safeguarded; adhere to this policy and should: alert their line manager or main most senior contact at the NSPCC where they believe the opportunity for fraud exists because of poor procedures or lack of effective supervision; report details of:

a) any suspected or actual fraud, or

b) any suspicious acts or events with their line manager, head of department or the Head of Governance, Risk and Compliance.

Alternatively, employees can use the NSPCC's 'Speak Up' (whistleblowing) policy (see link in paragraph 6) and assist in any investigations by making available all relevant information and by co-operating in interviews.

3. Procedure for raising a concern – Internal Reporting and the Fraud Response Plan

A Fraud Response Plan gives employees the details of the entire procedure for reporting any suspected fraud, defines the actions that the company needs to take and also defines authority levels, responsibilities for action, and reporting lines in the event of a suspected fraud or irregularity.

The procedure is described in Appendix A

4. Investigation

4.1. The NSPCC will take all reports of actual or suspected fraud, bribery and corruption seriously, and investigate proportionately and appropriately as set out in this policy and the Fraud Response Plan.

4.2. The Fraud Response Plan sets out responsibilities for investigating fraud, bribery and corruption, the procedures for investigating, action to be taken and external reporting.

4.3. Breach of this policy by employees will result in disciplinary action which could result in dismissal for gross misconduct.

5. Specific risk mitigation measures

5.1 To manage the exposure to bribery and corruption, all employees must comply with the Gifts and Hospitality policy and registration. This policy sets out how all employees (including consultants, agency and temporary employees), NSPCC Trustees and co-opted committee members must deal with offers of gifts and hospitality made or offered in the course of or related to their work at the NSPCC.

The policy covers: the key principles to be applied when considering whether any gifts and hospitality which may be offered by external individuals, bodies and organisations should be accepted; gifts and hospitality paid for by the NSPCC but received by employees, Trustees and co-opted committee members in the course of their work, eg meals at employee or board/committee meetings, conferences or training events; and the use of the Register of Gifts and Hospitality.

5.2 Conflicts of interest are known to increase the risk of fraud. Therefore, all employees must comply with the Conflict of Interest (Employee) policy. Any employee who believes they have an actual or potential conflict of interest (for example, using their position for personal benefit or gain or for the benefit or gain of someone closely connected with them) must advise their line manager and withdraw from the decision-making processes where their conflict arises. The register of interests is attached to Conflict of Interest (Employee) policy. This policy is applicable to all employees, agency staff, volunteers and contractors: a separate policy applies to NSPCC Trustees and co-opted Committee members.

Failure to report conflicts may result in disciplinary action.

6. Links to related NSPCC policies and procedures

- **Conflict of Interest (Employee) policy**

https://thegreen.nspcc.org.uk/Interact/Pages/Content/Document.aspx?id=2227&utm_source=interact&utm_medium=quick_search&utm_term=Conflict

- **Gifts and hospitality policy and registration**

https://thegreen.nspcc.org.uk/Interact/Pages/Content/Document.aspx?id=2230&utm_source=interact&utm_medium=quick_search&utm_term=Gifts

- **Internal Audit process, advice and investigations**

https://thegreen.nspcc.org.uk/Interact/Pages/Content/Document.aspx?id=2473&utm_source=interact&utm_medium=quick_search&utm_term=Internal+Audit+Process

- **Reporting Serious Incidents to the Charity Commission**

https://thegreen.nspcc.org.uk/Interact/Pages/Content/Document.aspx?id=2075&utm_source=interact&utm_medium=quick_search&utm_term=Reporting

- **NSPCC values-based behavioural framework**

https://thegreen.nspcc.org.uk/Interact/Pages/Content/Document.aspx?id=6063&utm_source=interact&utm_medium=quick_search&utm_term=NSPCC+value

- **Speak Up (Whistleblowing) policy**

https://thegreen.nspcc.org.uk/Interact/Pages/Content/Document.aspx?id=1760&utm_source=interact&utm_medium=quick_search&utm_term=Whistle

- **Disciplinary policy**

https://thegreen.nspcc.org.uk/Interact/Pages/Content/Document.aspx?id=1668&utm_source=interact&utm_medium=quick_search&utm_term=Disciplinary

7. Approval and review

Approved by	Audit & Risk Committee March 2022
Policy owner	Allison Howe, Head of Governance, Risk and Compliance |Society Secretary
Date	March 2024
Review date	March 2027

APPENDIX A

Anti-Fraud, Anti-Bribery and Corruption

THE FRAUD RESPONSE PLAN

Introduction

A Fraud Response Plan is aimed at ensuring that effective and timely action is taken in the event of fraud being alleged.

- Section 1 – details the response plan that applies to allegations of bogus fundraising for which there are particular steps.
- Section 2 - describes the response plan for any other fraud related incident alleged/suspected that is not covered in Section 1.

SECTION 1 - BOGUS FUNDRAISING RESPONSE PLAN

Please see the NSPCC intranet, the Green, link below:

https://thegreen.nspcc.org.uk/Interact/Pages/Content/Document.aspx?id=2466&utm_source=interact&utm_medium=quick_search&utm_term=Bogus

SECTION 2 - RESPONSE PLAN (all fraud related incidents not covered in Section 1).

HOW TO RAISE A CONCERN

Internal Reporting

If you suspect fraud, bribery or corruption including money laundering you must:

- immediately report suspicions to your line manager: if you do not feel comfortable doing this you may report your concerns to another manager or a director or to Internal Audit or the Head of Governance, Risk and Compliance;
- if you feel that your concerns have been wrongly dismissed, you may raise your suspicions with another manager or a director or Internal Audit or the Head of Governance, Risk and Compliance.

Line Managers

If you receive a report or suspect fraud, bribery or corruption including money laundering you must:

- immediately report it to your line manager or to Internal Audit or the Head of Governance, Risk and Compliance;
- Secure the relevant evidence as discretely as possible including IT equipment, revoke access where relevant.

Guidance on areas such as securing evidence, maintenance of confidentiality and how to report incidents is always available from Internal Audit or the Head of Governance, Risk and Compliance.

If you are unsure whether a particular act constitutes fraud, bribery or corruption, along with any other queries, these should be raised with your line manager or Internal Audit or the Head of Governance, Risk and Compliance.

External Reporting

A decision to refer suspected or attempted incidents of fraud or money laundering to the police will be made by the Chief Executive on the recommendation of the Head of Governance, Risk and Compliance. This decision will always be made in the best interests of children and young people.

Appendix B - Anti-Fraud, Anti-Bribery and Corruption Policy

FRAUD RISK ASSESSMENT – applicable to NSPCC Employees only

Challenges and Opportunities

On a periodic basis, annually as a requirement of each Directorate's Annual Assurance Statements that include submission of the Directorate's completed Fraud Risk Assessment. These are reported annually to the Finance, Audit & Risk Committee and Board of Trustees. Management should assess the organisation's exposure to fraud risk to identify potential fraud schemes and corruption risk events that need to be mitigated and monitored. An effective fraud risk assessment is tailored to the type of organisation and its unique activities. It should be performed on an annual basis and refreshed when a change in the internal or external environment occurs.

In line with the NSPCC Risks/Opportunities Management Policy, an effective fraud risk assessment methodology includes risk identification, assessment of inherent fraud risk (measured in terms of probability and significance/impact) and risk response. Fraud risk identification is best performed by gathering relative information on fraud risk from a variety of sources within the organisation and charity sector. This enables management to consider the totality of fraud risk threatening the organisation, as well as the impact of incentives, pressures, opportunities and rationalisation that lead to fraud.

Response to residual fraud risk should be balanced. Management's objective should be to implement effective anti-fraud controls, the benefits of which exceed their cost. Often, this involves a combination of manual and automated fraud prevention and detection techniques that enable the organisation to monitor for indicators of fraud within the scope of its risk tolerance.

Accepting that fraud risk exists within an organisation should not be an impediment to robust discussion of this threat. Authoritative guidance includes the premise that the risk of fraud occurs naturally within all organisations. Open and honest discussion about fraud risk through brainstorming, surveys and workshop activities should not be an organisational "taboo". In particular, it is important to note that because management has primary responsibility for the design, implementation and monitoring of internal controls, organisations are exposed to the danger of management override of controls. This is a key potential risk to consider during the fraud risk assessment process.

Conducting a fraud risk assessment

To protect the NSPCC, we need to be aware of any vulnerabilities that the NSPCC may be exposed to and strengthen our existing arrangements. This is why we need to conduct a robust **fraud risk assessment**, by following four simple steps.

Please see Table 2 - Fraud Risk Assessment form that can be populated to assist.

Step 1: Identify risks

Firstly, you need to assess your current operations and processes. To do this you could refer to historical data as well as emerging trends and patterns. Please see section headed 'Completion of Fraud Risk Assessments/Registers' below.

Step 2: Quantify risks

Estimate the probability and impact of each type of fraud. Use the probability/impact matrix to estimate the level of risk (see Table 1 below) along with your risk exposure. Please see section headed 'Completion of Fraud Risk Assessments /Registers' below.

Step 3: Mitigate risks

Once risks have been identified and quantified, you can use the 4T's model to mitigate them:

1. **Transfer** - in other words move the financial consequences to a third party. Generally, this involves getting insurance (the NSPCC has relevant insurance in place that is renewed annually);

2. **Terminate** - the simplest and most often overlooked solution. Stop doing things that are risky. This can be achieved through changes in practices and processes, or even by stopping engaging in activities with low reward and high risk;

3. **Treat** - here the aim is to reduce the probability and impact of risk. Again this could involve changes to systems and processes, but importantly this is where training teams about risk is vital.

4. **Tolerate** - this is the tricky area. You've found a risk, know its potential impact, but the cost of doing anything about it simply isn't worth it. This could include risks with low incidence (probability) and medium impact, or medium incidence (probability) and low impact. The NSPCC's 'risk appetite' is reviewed annually by the Board of Trustees.

Step 4: Monitor and review risks

It is important to see risk assessment as an ongoing process rather than a one off task. As part of the identify stage you will have already gained insights that will help you understand what to monitor and how to review. But new risks can appear, and the impact and prevalence of threats can change (both up and down). Think of your assessment like you would virus software, there to protect you and regularly in need of checking and updating. And that includes keep both your processes and your people up to date.

Completion of Fraud Risk Assessments/Registers

Fraud 'Project level' Risk Register - the key product of any Fraud Risk Assessment (FRA) is a fully populated 'project level' risk register. An organisation may have a number of these, covering individual payment / service / business areas. It may also have an overall one for the business, which is a combination of the key risks or high level/umbrella risks from the different areas. For example, within the Finance Directorate Risk Register.

Fraud Risk Assessment (FRA)

1. Fraud Risks/Registers should be clearly structured and accessible. Language used should be simple and understandable with minimal reference to other documents.

2. Statements should be based on evidence rather than based on assumptions. If assumptions are used these should be clearly acknowledged. For verification purposes, we need to state sources of evidence that can include the following: NSPCC & any other databases; files & drives where stored; documents and where can view them; and any third party evidence provided/referenced eg supplier/contractor information – that could be provided as part of procurement due diligence process, specify where can be viewed to verify and who has access to the information. See Table 2B.

3. The scope of the business area that the Fraud Risk covers and any areas that have been deemed out of scope should be clearly recorded.

4. If any risks, issues or controls are omitted from the Fraud Risk for reasons of sensitivity this should be clearly recorded.

5. Ideally an organisation would populate every field. However, there may be reasons why some columns may not be populated due to sensitivity. Where possible generic information should be included to aid management response.

6. In the final presentation, the Risk/Project Risk Register should be clearly structured and should be organised with the most important controls/risks first.

7. At the minimum, all prioritised risks/controls where additional mitigating action is being considered should have clearly defined owners in the business. All risks/controls in the risk would have clearly defined owners. These may be at individual risk level or in line with the structure for fraud risk agreed with the directorates. Where an owner cannot be identified, Internal Audit or the Head of Governance and Risk should direct where ownership should rest until senior management agree the responsible individual.

Assessing Inherent Risk of an Identified Fraud Risk

8. All Fraud Risks/Registers should have an assessment of the inherent risk that the risk poses. This is the risk posed if no controls/mitigating factors in place. The score rarely goes up unless external environment changes, eg political, legislative, economic etc.

9. The assessment of Inherent Risk should clearly assess the probability and impact of the risk occurring in the absence of the control framework.

10. All risks should be assessed and scored against the probability of their occurrence and the impact if they do occur.

11. A scoring system (see Table 1 below) of one to five (one being the lowest, five being the highest) should be used for both the probability and impact assessments. The Impact of the risk were it to materialise is weighted, therefore, the score is: Probability x Impact + *Impact*.

12. When assessing the probability and impact of a fraud risk, it is vital that scoring definitions that are meaningful for the risks are articulated. Where there are sensitive risks or controls that the organisation feels cannot be recorded in the overall FRA, there is an option to have a separate confidential FRA with limited circulation that considers these risks/controls.

<u>Fraud Risk Assessment</u>

13. Assessing the Identified Fraud Risk Current Risk Score – this is the current remaining/residual risk with the existing anti-fraud controls that are in place at the particular point in time and how far they mitigate the risk. When assessing probability, it should be acknowledged that fraud risks are often not limited to a single occurrence. The NSPCC's risk scoring system should be used that acknowledges that assessing fraud risk needs to consider both whether a risk will come to pass at all and also the frequency with which risks may occur. The result is a quantification of the risk.

14. When assessing corruption risks as part of a fraud risk assessment, the impact of corruption on both the frequency and probability should be considered. For example, the assessor should consider how collusion may affect the likely frequency of risks coming to pass (would it make it less likely to happen frequently), and whether it may make a risk more likely to succeed.

15. When assessing the impact of a risk the duration of any potential fraud should be considered alongside the potential impact of one-off occurrence. Consider if it is an operational risk occurring within 1 year, a project risk within the project timescales or a directorate/strategic risk covering 3 to 5 years. The Impact is weighted, therefore the overall score is Probability x Impact + *Impact* in order to focus on reducing the impact of the risk were it not mitigated sufficiently.

16. When assessing probability and impact all potential impacts of a fraud risk should be explored and understood. This is a creative process where impacts should be explored rather than assumed.

17. The mechanisms for capturing an organisation's view of probability and impact should remain consistent throughout the FRA process, in order to prevent the skewing of outcomes.

Please see the link below to the NSPCC Risks/Opportunities Management Policy on the intranet, the Green and the Volunteer Hub:

https://thegreen.nspcc.org.uk/Interact/Pages/Content/Document.aspx?id=1787&utm_source=interact&utm_medium=quick_search&utm_term=Risk+Management

TABLE 1 – FRAUD RISK ASSESSMENT/REGISTER SCORES

A. Probability-Impact Matrix – emphasising significance (PxI+I)

Probability

5	Almost certain	6	12	18	24	30
4	Likely	5	10	15	20	25
3	Possible	4	8	12	16	20
2	Unlikely	3	6	9	12	15
1	Rare	2	4	6	8	10
		Insignificant	Low	Medium	High	Extreme
		1	2	3	4	5

Impact

B. Probability Scales

Probability	Frequency Description	Approximate percentage range in next 12 months	Score
Rare	Extremely unlikely to happen	<5% very low probability	1
Unlikely	Unlikely to happen	5 – <15% low probability	2
Possible	Unlikely but could occur in the next 12 months	15 – <45% On balance unlikely to happen	3
Likely	Fairly likely to occur in the next 12 months	45 – <90% On balance likely to happen	4
Almost certain	Likely to occur in the next 12 months	>=90% high probability that will happen	5

D. Management Action Guide

Severity	Management Action & Escalation from Directorate to higher Strategic level
1 – 4	Low risk: Acceptable level of risk exposure, subject to regular monitoring
5 – 10	Moderate risk: Subject to regular active monitoring and requires measures to be put in place to reduce exposure. Risk should be escalated to a higher management level, for example, Senior Management Team
12 – 16	High risk: Subject to constant active monitoring and requires measures to be put in place to reduce exposure. Risk must be escalated to a higher management level, for example Senior Management Team or Executive Board and a dated note on the risk register as evidence of the context and reasonings of the relevant EB Director whether a Directorate Risk should or should not be considered for escalation on to the Strategic Risk Register prior to each FARC meeting.
18 – 30	Extreme risk: Unacceptable level of risk exposure, subject to constant active monitoring and requires immediate measures to be put in place to reduce exposure. Risk must be escalated to a higher management level, for example, Executive Board or Finance, Audit and Risk Committee. If in exceptional circumstances a risk with this Current Score is temporarily on a Directorate Risk Register, a dated note should be retained on the risk register as evidence of the context and reasonings of the relevant EB Director whether/when should or should not be escalated on to the Strategic Risk Register prior to each FARC meeting.

C. Impact scales

Impact	Objectives	Harm to a child or young person or vulnerable adult*	Service provision	Reputation	Health and Safety	Financial	People	Score
Insignificant			Minor/No impact on Children & Young People & Vulnerable Adults	No media interest	Minimal Injury	<£50k	Isolated to one of very small group of employees/volunteers	1
Low			Minor inconvenience which has a limited but not significant impact on Children & Young People & Vulnerable Adults	Local Media attention/with limited local impact/ complaint(s)	Minor reportable injury not	£50k – £1m	Small to medium group of employees/ volunteers affected	2

					requiring RIDDOR report			
Medium	Delay in meeting key corporate objectives		Children & Young People & Vulnerable Adults significantly impacted. A number of services affected	Adverse local media which impacts locally or a number of complaints. Brand damaged locally	RIDDOR reportable	£1m – £5m	Large group of employees/volunteers affected. Significant action required to remedy	3
High	General failure to meet objectives resulting in significant delay to implement strategy	Minor harm or injury suffered by a child or young person or vulnerable adult.	Significant impact on a large number of Children & Young People & Vulnerable Adults. Service might be suspended or reduced	Adverse national publicity and/or significant number of complaints. Impact on ability to influence Govt. Damage to brand	Specified injury/ illness. Might affect more than one person. Possible enforcement action by HSE	£5m – £15m	Significant group of employees/volunteers affected resulting in disruption in the workplace, or significant under performance, loss of key skills. Inability to attract and retain talent	4
Extreme	Objectives which are identified as key to organisational effectiveness are not achieved or the strategy is not implemented	Harm or injury suffered by a child or young person or vulnerable adult.	Service suspended/ stopped/ delayed which has a significant long term effect on a large number of Children & Young People & Vulnerable Adults and may put Children & Young People & Vulnerable Adults at risk of harm	Adverse sustained national publicity resulting in loss of public or political confidence. Significant impact on ability to influence Govt. Brand tarnished to the extent that re-branding may be necessary	Loss of Life/ Major incident which is more than likely as a result negligence or which could lead to prosecution	>£15m	Large numbers of employees/volunteers leave or threaten to leave which significantly impacts on operational effectiveness, and results in loss of vital skills and knowledge. Significant under performance affecting whole organisation. Significant inability to retain and attract talent	5

***Vulnerable Adult includes Adult at Risk**

Table 2 – FRAUD RISK ASSESSMENT FORM (applicable to relevant employees only)

When conducting the Fraud Risk Assessment please ensure you consult the Anti-Fraud, Anti-Bribery and Corruption Policy (the Policy) AND the accompanying training slides (includes examples of fraud risks) that are on the Green.

Please complete both Tables 2A and 2B below.

NAME OF DIRECTORATE: [ ]

Completed/certified by: [ ]

Job title: [ ]

Date: [ ]

TABLE 2A – to be completed

	Identified Fraud risks *(for each risk identified, please also complete Table 2B below)*	**Inherent Risk Score** *(the risk posed if no controls /mitigating factors in place)*			**Current Risk Score** *('residual' ie current risk remaining with the existing anti-fraud controls)*			**Employees with overall responsibility (full name & job title/role) and** **Department/any third party details**	**Existing Anti-fraud Controls** *(should be *SMART)* **& named Control Owners**	**Controls Effectiveness Assessment** *this should relate to the Current Score* Effective/ Partially Effective/ Not Effective/ OR N/A – provide Explanation	**Fraud Risk Response** Transfer/ Terminate/ Treat/ Tolerate	**Action(s) required** *(numbered)* *(should be *SMART)*	**Action(s) Control Owner + Due Dates** *(numbered)* **& confirm when completed**
		P	**I**	**PxI+I**	**P**	**I**	**PxI+I**					i)	i)
1													
2													
3													
4													
5													
6													
7													

**SMART = specific, measurable, achievable, relevant & time-bound. Controls should be 'SMART' – anything that helps to: a) reduce the probability of the risk occurring &/or b) reduce the impact of the risk. It should be capable of being audited with evidence provided including procedure to monitor & test efficacy.*

TABLE 2B – to be completed for *EACH IDENTIFIED FRAUD RISK* in TABLE 2A above:

No.	Identified Fraud Risk	Methodology used in conducting the fraud risk assessment How risk identified - eg types of meetings, one individual, group discussions, surveys, workshop activities etc	List sources of information to evidence the effectiveness of existing controls - to be available on request for verification purposes Eg specify NSPCC databases, files & drives where stored, documents and where can view them, & any third party evidence provided/referenced eg supplier/contractor information – that could be provided as part of procurement due diligence process, specify where can be viewed to verify.
1			
2			
3			
4			
5			
6			
7			