Anti-Fraud and Corruption Policy

Last Reviewed: September 2026
Next Review: August 2027
Cycle: Annual
Version: 1.0

Tel: 01709 914070 | Email: admin@stfranciscmat.com | www.stfcmat.com
Registered Office: The Old Grammar School, 13 Moorgate Road, Rotherham, S60 2EN

Contents

Changes to this Edition	
Statement of Intent	
1.0	Legal Framework
2.0	Definitions
3.0	Roles and Responsibilities
4.0	Indicators for Potential Fraud
5.0	Creating an Ethical Culture
6.0	Preventing Fraud
7.0	Record Keeping
8.0	Gifts and Hospitality
9.0	Reporting Concerns and Making Allegations
10.0	Investigating Reports
11.0	Reporting to the DfE
12.0	Following an Investigation
13.0	Cyber-crime and Cyber-security
14.0	Money Laundering
15.0	Confidentiality
16.0	Annual Accounts
17.0	Monitoring and Review
Appendix A	Indicators for Potential Fraud

Changes to this Edition

DATE	VERSION	DETAILS OF CHANGES
November 2025	1.0	Frist Edition – using National College Template
September 2026	2.0	No Changes

Statement of intent

St Francis Catholic Multi Academy Trust is committed to operating with the highest ethical standards and acting with integrity in all activities. The risks of fraud, theft, irregularity and cyber-crime are taken seriously, and proportionate controls will be implemented to mitigate the risks.

This policy sets out our responsibilities regarding the prevention of fraud and corruption, and the promotion of an ethical culture. The policy also sets out the procedures that will be followed where fraud or corruption are discovered or suspected.

1.0 Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Public Interest Disclosure Act 1998
- Terrorism Act 2000
- Proceeds of Crime Act 2002
- Fraud Act 2006
- Companies Act 2006
- Bribery Act 2010
- Charities Act 2011
- DfE (2025) 'Reducing fraud in the education sector'
- DfE (2025) 'Academy trust handbook 2025' (ATH)

This policy operates in conjunction with the following school policies:

- Whistleblowing Policy
- Finance Policy
- Gifts, Hospitality and Anti-bribery Policy
- Conflicts of Interests Policy
- Disciplinary Policy and Procedure
- Staff Code of Conduct
- Board of Trustees Code of Conduct
- Cyber-security Policy

2.0 Definitions

Fraud is a criminal offence, which is defined in the Fraud Act 2006 as:

- Deceiving through false representation.
- Failing to disclose information where there is a legal duty to do so.
- Abusing a position of trust.

Corruption is the offering, giving, soliciting or accepting of any inducement or reward which may influence the actions taken by the body, its members or officers.

Theft is dishonestly appropriating property belonging to another with the intention of permanently depriving the other of it.

Bribery is defined by the Bribery Act 2010 as inducement for an action which is illegal, unethical or a breach of trust. Inducements can take the form of gifts, loans, fees, rewards or other advantages.

In this policy, 'fraud' will be used to refer to all the definitions outlined above.

Examples of what could constitute fraud include, but are not limited to, the following:

- Theft of cash
- Substitution of personal cheques for cash
- Travelling and subsistence claims for non-existent journeys or events, or inflating claims
- Manipulating documentation to increase salaries
- Payment of invoices for goods received by an individual rather than the trust
- Unauthorised borrowing of equipment
- Failure to declare a conflict of interest
- Concealing a generous gift or reward

- Creation of false documentation

3.0 Roles and responsibilities

Overall responsibility for dealing with fraud lies with the accounting officer. Responsibilities of the accounting officer will include:

- Overseeing the development and implementation of a system of internal controls that aim to minimise the risk of fraud.
- Overseeing the financial transactions and the development and implementation of effective financial regulations, policies and procedures to prevent losses and misuse.
- Ensuring bank accounts, financial systems and financial records are operated by more than one person.
- Ensuring resources are being managed in an ethical, efficient and economical manner.
- Ensuring that rigorous investigations of potential fraud are carried out promptly.
- Ensuring the appropriate legal and/or disciplinary action is taken where fraud is proven.
- Ensuring that appropriate action is taken to recover assets and minimise loss.
- Keeping full and accurate accounting records and producing the trust's annual accounts, including a statement on regularity, propriety and compliance.
- Advising the board of trustees in writing if action it is considering is incompatible with the Articles of Association, funding agreement or ATH, and notifying the DFE's accounting officer if the board proceeds with action considered to be in breach.

The board of trustees will appoint, in writing, a senior executive leader, who may be appointed as a trustee.

The trust will ensure that the senior executive leader is named as the appointed accounting officer. The roles of senior executive leader and accounting officer will not rotate. The trust will not appoint the CFOO as the accounting officer.

The external auditor will be responsible for certifying whether the trust's annual accounts present a true and fair view of its financial performance and position.

The CFO will be responsible for:

- Assessing the areas of the trust that are most vulnerable to fraud, in conjunction with the headteacher.

- Conducting an initial investigation where a report of fraud is made, in conjunction with the headteacher.
- Contacting the DFE to request prior approval for any transactions beyond the trust's delegation limits, and transactions that are novel, contentious or repercussions.

The chair of trustees will be responsible for:

- Receiving reports of fraud that involve the headteacher.
- Ensuring the DFE is notified as soon as possible in relation to instances of fraud, theft and irregularity in line with section 11 of this policy.

The headteacher will be responsible for:

- Assessing the areas of the trust that are most vulnerable to fraud, in conjunction with the CFOO.

- Receiving reports of fraud.
- Conducting an initial investigation where a report is made, in conjunction with the CFOO. ▪

Approving gifts and hospitality in line with the Gifts, Hospitality and

Anti-bribery Policy. ▪ Ensuring employees are provided with appropriate anti-fraud training.

- Maintaining the Conflicts of Interests Register and Gifts and Hospitality Register.

The audit and risk committee will be responsible for reviewing the trust's internal controls, and for conducting a full investigation of reports and determining what the next steps will be.

The board will identify and demonstrate sufficient financial knowledge to hold the setting's executives to account.

All employees (including volunteers and temporary staff) and third parties that work with the trust will be responsible for:

- Demonstrating the highest standards of honesty, probity, openness and integrity in the discharge of their duties.

- Complying with the provisions outlined in this policy.
- Being vigilant to the risks and indicators of fraud.
- Promoting an ethical, anti-fraud culture.
- Reporting their concerns in relation to fraud to the headteacher or chair of trustees.
- Reporting any breach of this policy to the headteacher or accounting officer.
- Providing information about any conflicts of interest and direct or indirect pecuniary interests to the headteacher.
- Maintaining the academy trust's estate in a safe working condition.

Management accounts which set out the trust's financial performance and position are prepared every month and shared with the chair of trustees every month. The trust board will consider management accounts when it meets.

Appropriate and timely action will be ensured by the board to maintain financial viability.

Where the trust sees fit, it will amalgamate its General Annual Grant (GAG) from one central

fund.

4.0 Indicators for potential fraud

Some actions and behaviours may give cause for concern, arouse suspicion and possibly indicate fraudulent activity. These are outlined in appendix A. The list provided in appendix A is not exhaustive; fraud can take many different forms. All employees will be vigilant to the indicators of fraud.

Clarification will be sought from the headteacher or CFOO if there are any questions over whether something could be considered an indicator of fraud. The presence of any of these indicators may not be a cause for concern; however, they will always be investigated appropriately in accordance with section 10 of this policy.

5.0 Creating an ethical culture

An ethical, anti-fraud culture will underpin all the work done by the trust to counter fraud. All employees and third parties that work with the trust will be expected to act with high levels of integrity and to adhere with the rules outlined in this policy.

Overarching anti-fraud awareness training will be held for all employees on an annual basis. Role-specific training will also be provided to employees with responsibility for the trust's internal controls or financial procedures on an annual basis or when a procedure changes.

Employees will be encouraged to report any concerns, and clear reporting mechanisms will be implemented and communicated. Victimisation or harassment of anyone who has made a report will not be tolerated.

6.0 Preventing fraud

The headteacher and CFOO will assess the areas of the trust that are most vulnerable to fraud risks on an annual basis. Fraud risks will be identified for all areas and processes of the trust and will be assessed in terms of impact and likelihood. Both monetary and non-monetary impacts will be considered, such as the impact on the trust's reputation.

Robust internal controls will be put in place to manage the risk of fraud – these will cover areas including the following:

- Process of authorising transactions
- Access restrictions and transaction controls
- Account reconciliations
- Physical security of assets
- Segregation of responsibilities
- Pre-employment checks

All employees that are involved in the implementation of these controls will be provided with relevant training. Internal controls will be reviewed on an annual basis by the finance committee, in conjunction with the headteacher, to ensure they remain effective and are being consistently applied.

All employees will follow the Staff Code of Conduct and will be required to declare any business or pecuniary interests, or other conflicts of interest, to the headteacher. Trustees will be required to declare conflicts of interest to the chair of trustees.

Following a case of fraud, the risk management strategy will be reviewed to ensure it considers all relevant risks and that the internal controls are effective.

7.0 Record keeping

Financial records will be kept, along with evidence for the business reasons for making payments to third parties.

Employees will be required to make the headteacher aware of all gifts or hospitality received or offered over the value of £25; these will be subject to review. Employees' expenses claims relating to gifts, hospitality or expenses incurred to third parties will be submitted in accordance with the Staff Expenses Policy.

All invoices, accounts and related documents will be prepared and maintained will the highest accuracy and completeness. No accounts will be kept "off-book" and any reports of fraud, and subsequent investigations, will be recorded.

The trusts will no longer need to provide an explanation when the board has not met at least six times in the academic year in their governance statement.

The academy trusts will submit an 'Academies budget forecast return' to the DFE by the end of August.

8.0 Gifts and hospitality

It is not acceptable for employees to:

- Give, promise or offer payment, gifts or hospitality, with the expectation or hope that an advantage for the trust will be received or to reward an advantage already received.

- Give, promise or offer a payment, gift or hospitality to a government official, agent or representative to facilitate or expedite a routine procedure.

- Accept payment from a third party if they know or suspect that it is offered with an expectation of a business advantage in return.

- Threaten or retaliate against another employee who has refused to commit a bribery offence or who has raised concerns regarding bribery.

- Engage in any activity that may lead to a breach of the Gifts, Hospitality and Anti-bribery Policy.

The trust will not prohibit normal and appropriate hospitality or gifts (both given and received) if the following requirements are met:

- It is not made with the intention of influencing a third party to obtain or retain business or business advantage, or to reward the provision or retention of business or business advantage, or in exchange for favours or benefits
- It is given in the trust's name, not the individual's name
- It complies with the law
- It does not include cash or a cash equivalent, e.g. vouchers or gift certificates
- It is appropriate in the circumstances, e.g. the giving of small gifts at Christmas
- The type and value of the gift is reasonable given the reason the gift is offered
- It is given openly, not secretly

Gifts should not be offered to, or accepted from, government officials or representatives without the prior approval of the headteacher. In all circumstances, employees should consider whether the gift or hospitality is reasonable and justified and consider the intention behind the gift.

Any gifts and hospitality given or received will be recorded on the Gifts and Hospitality Register.

9.0 Reporting concerns and making allegations

Any allegations or concerns of suspected fraud will be reported to the headteacher. Allegations involving the headteacher will be reported to the chair of trustees. Allegations involving governors or trustees will be made to the accounting officer.

Third parties will report any concerns to the headteacher or the chair of trustees, depending on what the allegation involves. Any person with a concern or allegation will not investigate the matter themselves.

Procedures outlined in the Whistleblowing Policy can be followed to report concerns. Employees, volunteers and third parties will be made aware that reports can also be made directly to the DFE using an online form here.

Tel: 01709 914070 | Email: admin@stfranciscmat.com | www.stfcmat.com
Registered Office: The Old Grammar School, 13 Moorgate Road, Rotherham, S60 2EN

10.0 Investigating reports

Reports will be initially investigated by the headteacher and CFOO, who will ascertain the facts of the report, seeking HR and legal advice as necessary. The headteacher will notify the chair of trustees of any serious financial irregularities at the first opportunity following the completion of an initial investigation.

Following the initial investigation, the matter will be reported to the audit and risk committee who will undertake the management of the investigation. When a report has been escalated to the audit and risk committee, the individual(s) the allegation has been made against will be informed of the investigation. They will not be informed of who made the allegation.

In undertaking an investigation of a report, the audit and risk committee will:

- Conduct an investigation to gather factual information and reach an initial view as to whether further action is required.
- Collect relevant evidence, interview all relevant people and analyse any related documentation.
- Decide if the evidence suggests that the allegation or concern is proven.
- Recommend any changes to the internal controls in light of the findings.
- Determine whether the findings, conclusions and any recommendations arising from the investigation should be reported to the chair of trustees.
- If further investigations are required, determine which outside agencies should be involved, e.g. auditors or the police.

The audit and risk committee will, where possible, quantify any potential or actual financial loss and ensure steps are taken at an early stage to prevent further loss occurring. The audit and risk committee will notify the trust's external auditor of any cases it is investigating, and of the outcome of these cases.

All concerns and reports will be taken seriously and investigated in line with the process outlined above. Reporters will be asked to provide any evidence they have to support their allegations. Any person who makes a report will be reassured that they will not suffer recrimination as a result of raising any reasonably held suspicion.

Reports will be investigated objectively; the facts will be considered as they appear, based on the information to hand. Individuals about which a report is made will not be accused or approached directly prior to an investigation.

11.0 Reporting to the DFE

The chair of trustees will report any instances of fraud, theft and/or irregularity exceeding £5,000 individually, or £5,000 cumulatively in any financial year, to the DFE as soon as possible. Unusual or systematic fraud, regardless of value, will also be reported. When making a report to the DFE, the accounting officer will provide the following information:

- Full details of the event(s) with dates
- The financial value of the loss
- Measures that have been taken to prevent recurrence
- Whether the matter was referred to the police, and, if not, the reasoning behind this
- Whether insurance or the risk protection arrangement (RPA) have offset any loss

Following a report, the DFE may conduct or commission its own investigation into actual or potential fraud, theft or irregularity in the trust, either as a result of a notification from the trust or from other information the DFE has received. Other authorities, including the police, may be involved in the investigation.

The trust will obtain the DFE's prior approval for the supply of goods or services to the trust agreed on or after 1 September where a contract or other agreement exceeds £40,000 in the same financial year ending on 31 August. This approval process will not apply when contracts or agreements for goods or services are arranged between the trust and the following establishments:

- Colleges, universities and schools that are sponsors of the academy trust
- State-funded schools and colleges, including academies

12.0 Following an investigation

The trust will seek to apply appropriate criminal, civil and disciplinary sanctions to all cases of proven fraud and corruption. Where fraud involving an employee is proven, this constitutes as gross misconduct and cases will be dealt with accordingly in line with the Disciplinary Policy and Procedure.

The trust may terminate the contracts of any third party or other associated person acting on behalf of the trust where they are found to have breached this policy. Disciplinary action may be taken against employees that make malicious reports of fraud.

Where appropriate, cases will be referred to the police in order for them to consider taking criminal action.

Following any incident of fraud, a 'lessons learned' exercise will be conducted. All individuals involved in the investigation of the case will be involved in the activity, which will aim to identify areas of internal controls or other procedures that should be improved to prevent further cases occurring.

13.0 Cyber-crime and cyber-security

The trust will be vigilant to cyber-crime and clear cyber-security measures and proportionate controls will be implemented, as outlined in the Cyber-security Policy. Appropriate action will be taken where a cyber-security incident occurs, in line with the trust's Cyber Response and Recovery Plan.

The following measures will be implemented specifically relating to addressing the risk of fraud:

- Firewalls, anti-virus software and strong passwords will be used
- Data will be routinely and securely backed up
- A restricted number of devices will be used to access financial or other

sensitive data Staff will receive training to ensure they:

- Check the sender of an email is genuine before, for example, sending payment data or passwords.
- Make direct contact with the sender where an email requests a payment – this will be done in person where possible, but at a minimum staff must use another method other than the direct reply function, such as a phone call.
- Understand the risks of using public WiFi.
- Understand the risks of not following payment checks and measures.

Any suspected incidents of fraud relating to cybersecurity will be reported and investigated as outlined in section 9 and section 10 of this policy.

The trust will follow the National Crime Agency's (NCA) recommendation to not pay cyber ransom demands. Any decision to pay a cyber ransom demand will only be made if permission has been obtained from the DFE.

14.0 Money laundering

"Money laundering" describes offences concerning the possession, concealment, conversion, transfer or making of arrangements relating to the proceeds of crime. This is not limited to money or cash.

Trustees will take appropriate and reasonable steps to ascertain where funds received by the trust come from. This includes:

- Identifying who they are dealing with.
- Verifying identities, where appropriate, and there are high risks.
- Checking the nature of the organisations or individual's business to be assured that this is appropriate for the trust to be involved with.
- Watching out for unusual, complex or suspicious activities, conduct or requests.
- Ensuring that any conditions attached to receiving the funds are appropriate and can be accepted and there is reasonable assurance that the funds are not from any illegal or inappropriate source.

All decisions by trustees to accept or refuse donations will be recorded in writing in order to demonstrate that decisions were taken responsibly, with due consideration given to any risks.

Payments by cash will only be accepted by the school up to a value of £500 from known individuals and organisations.

Any concerns held by staff relating to money laundering will be raised with the accounting officer. Where the trust knows or suspects that an individual or organisation is engaged in money laundering or dealing in criminal property, the accounting officer will submit a suspicious activity report (SAR) to the NCA. The individual or organisation the report concerns will not be informed of the suspicion. Careful consideration will be given to the trust's relationship with the individual or organisation once the report has been submitted.

15.0 Confidentiality

The trust understands that the decision to report a concern can be a difficult one to make. Victimisation or harassment of anyone who has made a report will not be tolerated.

Where possible, the identity of the person who made the report will be kept confidential; their identity will only be shared on a need-to-know basis. The identity of the individual(s) about whom an allegation is made will be also be kept confidential, and only shared on a need-to-know basis. Where an allegation is proven to

be unfounded or malicious, the individual about whom the allegation was made will be provided with appropriate support.

16.0 Annual accounts

The accounting officer will submit the trust's annual accounts return to the DFE each year. These accounts will include the accounting officer's statement on regularity, propriety and compliance.

The accounting officer will include any identified cases of fraud in the statement. The annual audited accounts will be:

- Submitted to the DFE by 31 December each year.
- Published on the trust's website by 31 January.
- Filed with Companies House in accordance with company law requirements, usually by 31 May.
- Provided to anyone who requests a copy.

The external auditor will certify whether the annual accounts present a true and fair view of the trust's financial performance and position.

17.0 Monitoring and review

This policy will be reviewed on an annual basis by the Trust. The next scheduled review date for this policy is August 2026.

Any changes made to this policy will be communicated to all employees and third parties that work with the trust.

The next scheduled review date for this policy is **August 2027**.

Appendix A - Indicators for potential fraud

Personal motives for fraud

- Personnel believe they receive inadequate compensation and/or rewards, e.g. recognition, job security, holidays or promotions
- Expensive lifestyle, e.g. cars and holidays
- Personal problems, e.g. gambling, alcohol, drugs or debt
- Unusually high degree of competition or peer pressure
- Related party transactions (business activities with personal friends, relatives or their companies)
- Conflicts of interest
- Disgruntled employee, e.g. being recently demoted or reprimanded
- Recent failure associated with specific individual
- Personal animosity or professional jealousy

Organisational motives for fraud

- Organisation experiencing financial difficulty
- Commercial arm experiencing financial difficulty
- Tight or unusually tight time deadlines to achieve level of outputs
- Organisational governance lacks clarity, direction or substance
- Organisation closely identified with, or dominated by, one individual
- Organisation under pressure to show results, e.g. budgetary matters or exam

results

▪ Organisation recently suffered disappointment or consequences of bad decisions ▪

Organisation wants to expand its scope or obtain additional funding

▪ Funding award or contract for services is up for renewal or continuation

▪ Organisation due for a site visit by auditors, Ofsted or others

▪ Organisation has a for-profit component

▪ Organisation recently affected by new and/or changing conditions, e.g. regulatory, economic or environmental

▪ Organisation faces pressure to use or lose funds to sustain future funding levels

▪ Record of previous failure(s) by one or more organisational areas, associated business or key personnel

▪ Sudden change in organisation practice or pattern of behaviour

Weakness in internal controls

▪ There is a general lack of transparency about how the organisation works, and its procedures and controls

▪ Management demonstrates a lack of attention to ethical values – including a lack of communication regarding the importance of integrity and ethics, a lack of concern about the presence of temptations and inducements to commit fraud, a lack of concern regarding instances of fraud, and no clear fraud response plan or investigation policy

▪ Management fails to specify and/or require appropriate levels of qualifications, experience or competence for employees

▪ Management displays a penchant for taking risks

▪ Lack of an appropriate organisational and governance structure with defined lines of authority and reporting responsibilities

▪ Organisation lacks policies and communication relating to individual accountability and best practice, e.g. related to procurement, expenses, use of alcohol and declarations of interest

- Lack of personnel policies and recruitment practices
- Organisation lacks personnel performance appraisal measures or practices
- Management displays a lack of commitment towards the identification and management of risks relevant to the preparation of financial statements
- There is inadequate comparison of budgets with actual performance and costs, forecasts and prior performance – there is also no regular reconciliation of control records and a lack of proper reporting to the board of trustees
- Management of information systems is inadequate, e.g. no policy on ICT security, computer use, verification of data accuracy, or completeness or authorisation of transactions
- There is insufficient physical security over facilities, assets, records, computers, data files and cash
- Failure to compare existing assets with related records at reasonable intervals
- There is inadequate or inappropriate segregation of duties regarding initiation, authorisation and recording of transactions, maintaining custody of assets, and alike
- Accounting systems are inadequate, i.e. they have an ineffective method for identifying and recording transactions, no tracking of time periods during which transactions occur, insufficient description of transactions and to which account they should be allocated to, no easy way to know the status of funds on a timely basis, no adequate procedure to prevent duplicate payments, or missing payment dates
- Purchasing systems and/or procedures are inadequate, e.g. poor or incomplete documentation to support procedure, purchase, payment or receipt of goods or services
- Subcontractor records and/or systems reflect inadequate internal controls
- There is a lack of internal, ongoing monitoring of controls which are in place and/or failure to take any necessary corrective actions
- Management is unaware of or displays a lack of concern regarding applicable laws, e.g. Companies Act, Charities Act
- Specific problems and/or reportable conditions identified by prior audits or other means of oversight have not been corrected
- No mechanism to exists to inform management, directors, trustees or governors of possible fraud

- General lack of management oversight

Transactional indicators

- Related party transactions with inadequate, inaccurate, or incomplete documentation or internal controls, e.g. business activities with friends
- Not-for-profit entity has for-profit counterpart with linked infrastructure, e.g. shared board of trustees, governors or other shared functions and personnel
- Specific transactions that typically receive minimal oversight
- Previous audits with findings of questioned costs, evidence of non-compliance with applicable laws or regulations, weak internal controls, a qualified audit opinion, or an inadequate management response to any of these issues
- Transactions and/or accounts which are difficult to audit and/or subject to management judgement and estimates
- Multiple sources of funding with inadequate, incomplete or poor tracking, failure to segregate funds, or existence of pooled funds
- Unusual, complex or new transactions, particularly if they occur at year end or end of reporting period
- Transactions and accounts operating under time constraints
- Cost sharing, matching or leveraging arrangements where industry money or other donation has been put into a foundation without adequate controls to determine if money or equipment has been spent or used and whether it has gone to allowable costs and at appropriate and accurate valuations
- Outside entity provided limited access to documentation
- Travel accounts with inadequate, inaccurate or incomplete documentation or poor internal controls, variances between budgeted amounts and actual costs, claims in excess of actual expenses, reimbursement for personal expenses, claims for non-existent travel, or collecting duplicate payments

- Credit card accounts with inadequate, inaccurate or incomplete documentation or internal controls such as appropriate authorisation and review
- Accounts in which activities, transactions or events involve handling of cash or wire transfers
- Presence of high cash deposits maintained with banks
- Assets which are of a nature easily converted to cash (e.g. small size, high value, high marketability or lack of ownership identification) or easily diverted to personal use (e.g. cars or houses)
- Accounts with large or frequent shifting of budgeted costs from one cost centre to another without adequate justification
- Payroll (including fringe benefits) system has inadequate controls to prevent an individual being paid twice or paid for non-delivery or non-existence
- Payroll (including fringe benefits) system is outsourced but there is poor oversight of starters, leavers and payments
- Consultant and subcontract agreements which are vague regarding the work, time period covered, rate of pay or product expected
- There is a lack of proof that a product or service was actually delivered by a consultant or subcontractor
- Sudden and/or rapid growth of newly contracted or existing education providers, e.g. significant increase in pupil numbers for newly contracted providers

Methods used to commit and/or conceal fraud

Employee indicators such as:

- Eagerness to work unusual hours
- Access to or use of computers at unusual hours
- Reluctance to take leave or seek support

- Insistence on doing their job alone
- Refusal of promotion or reluctance to change their job

Auditor or employee issues such as:

- Refusal or reluctance to provide information or hand over documents
- Unreasonable explanations
- Annoyance or aggressive responses to questions or requests, in an attempt to deter auditors
- Trying to control the audit process
- Employee blames a mistake on a lack of experience with financial requirements or regulations governing funding
- Promises of cooperation followed by subsequent excuses to limit or truncate cooperation
- Subtle resistance
- Answering a question that was not asked
- Offering more information than asked
- Providing a lot of information in some areas and little to none in others
- Explaining a problem by saying “we’ve always done it that way”, “someone from the government told us to do it that way” or “Mr X told us to do it that way”
- A tendency to avoid personal responsibility, e.g. overuse of “we” and “our” rather than “I”
- Blaming someone else
- Too much forgetfulness
- Trying to rush the audit process
- Uncharacteristic willingness to settle questioned costs in an attempt to deter further investigation or analysis

General indicators such as:

▪ A general lack of transparency about how the organisation works and its procedures and controls

▪ Fabricated explanations to support inability or unwillingness to evidence transactions or assets, such as stated loss of electronic data or theft of business records **Record keeping, banking and other**

▪ Documents that are missing, copied, written in pencil, altered, or that contain false signatures, the incorrect signature or no authorisation where it would be expected

▪ Deviation from standard procedures, e.g. all files but one handled in a particular way

▪ Excessive and/or poorly evidenced journal entries, unable to provide explanation for journal entries

▪ Transfer to or via any type of holding or suspension account

▪ Inter-fund company loans to other linked organisations

▪ Records maintained are inadequate, not updated or not reconciled

▪ Use of several different banks or frequent bank changes

▪ Use of several different bank accounts

▪ Failure to disclose unusual accounting practices or transactions

▪ Unusual accounting practices or transactions, including

Uncharacteristic willingness to settle questioned costs

Non-serial-numbered transactions or out-of-sequence invoices or other documents

- Creation of fictitious accounts, transactions, employees or charges
- Writing large cheques to cash or repeatedly to a particular individual
- Excessive or large cash transactions
- Payroll cheques with unusual or questionable endorsements

- Payees have similar names or addresses

- Non-payroll cheques written to an employee

▪ Defining delivery needs in ways that can only be met by one source or individual

▪ Continued reliance on person or entity despite poor performance

▪ Treating non-business and/or personal goods or services as business transactions in financial records

▪ Misuse of directors' loan account facility, e.g. deliberate miscoding of transactions in directors loan account to gain personal advantage

▪ Materials, goods and or services fictitiously erroneously reported as purchased, and evidence has been fabricated to support the claim. This could potentially be evidenced by:

- Repeated purchases of the same items
- Identical items purchased in different quantities within a short time period
- Invoices and statements used to evidence purchase facilitating duplicate transactions or payments
- Anomalies in the format of purchase invoices
- Goods or equipment are not used as promised, or they do not work or exist
- Legitimate business assets put to non-business or private use