Anti-Fraud Policy and Response Plan

Policy owner	Director of Finance
Approving board/ committee	RHT Board
Date approved	July 2026
Date implemented	1 September 2026
Review period	3 Years
Next review due	Summer 2029

Contents

1 Policy Statement

1.1 Introduction

The purpose of this Policy is to outline our approach, as well as defining roles and responsibilities, for dealing with the threat of fraud and corruption, both internally and externally. It applies to Members, Trustees, Academy Governors, staff, students, suppliers, contractors, consultants, and other service users.

In compiling this policy, we have taken into consideration the DfE Fraud Awareness: good practice for education and training provider guidance that covers, the Economic Crime and Corporate Transparency Act 2023 (came into force September 2025) and the Fraud Act 2006. In addition, we have included the requirements of the Academy Trust Handbook in relation to fraud prevention and notification.

- We are committed to protecting the public funds with which we have been entrusted. It is essential that losses due to fraud and corruption are minimised to ensure resources are used for their intended purpose of providing education
- The public and our funding bodies are entitled to expect us to conduct our affairs with integrity, honesty and openness and demand the highest standards of conduct from both staff and students. This Anti-Fraud Policy outlines our commitment to creating an anti-fraud culture and maintaining high ethical standards in our administration of public funds
- We have a zero tolerance to any form of fraud.
- Other Trust policies that are inter-related to this policy include:
    - Staff and student code of conduct
    - Whistleblowing
    - Risk management
    - Conflicts of interest
    - Cyber incident response plan
    - Declaration of interests
    - Financial regulations and procedures
    - Gifts and Hospitality
    - Disciplinary
    - Anti-bribery and corruption

1.2 Culture

- We believe that the creation of a culture of honesty and openness is a key element in tackling fraud, as is raising the level of awareness and understanding of the key policies and procedures and their role in preventing or detecting fraud. In our commitment to maintaining the highest standards of governance, we have defined acceptable behaviour which both staff and students are expected to follow. These are based on the Nolan Principles of Standards in Public Life.
- Our staff and students are an important element in our stance on fraud and corruption, and they are encouraged to raise any concern that they may have on these issues where they are associated with our business or activity.

1.3 Definitions of Fraud and its impact

The Fraud Act 2006 defines fraud as:

- fraud by false representation – where a person expresses or implies something, which they know to be untrue or misleading.
- fraud by failing to disclose information – where a person fails to disclose information, which they have a legal duty to disclose.
- fraud by abuse of position – where a person is in a position where they are expected to safeguard the financial interests of others but abuse that position.
- In considering what constitutes fraud, there are a number of related concepts that are often talked about alongside fraud, these are:

- bribery – the giving, offering, receiving, or soliciting of something of value as a means to influence the actions of an individual or organisation in a position of power
- corruption – the abuse of entrusted power for private benefit that usually breaches laws, regulations, standards of integrity and or standards of professional behaviour
- theft – the dishonest appropriation of property belonging to another with the intention to permanently deprive the other of it
- error, a misstatement that is unintentional and does not involve deliberate deception
- irregularity – acts of omission or commission, either intentional or unintentional, which are contrary to the prevailing laws or regulations and can include fraud

Fraud is a general term covering theft, deliberate misuse or misappropriation of assets or anything that leads to a financial advantage to the perpetrator or others upon whose behalf they act, even if these "others" are in ignorance of the fraud. Fraud is intentional deceit and for this reason we do not consider negligence as fraud.

Fraud can have far-reaching consequences that can be long lasting. The DfE guidance sets out four areas of potential impact

- **Financial**
  The most obvious impact is financial where significant sums of money are lost to fraudsters. In the education sector an example could be where a provider is tricked into paying a fake invoice.
- **Reputational**
  Losing money to a fraud can be reputationally damaging for an organisation as it erodes trust in its processes and systems. In the education sector this could result in providers finding it harder to receive favourable terms from suppliers, lenders, funders, donors and grant providers. It could also impact on third parties wanting to contract with them, learners wanting to study with them, and people seeing them as a good employer to work for.
- **Societal**
  Where public funds are lost to fraud it means less money is available to government to spend on public services as a whole.
- **Human**
  The human impact of fraud can be devastating and traumatic when individuals become a victim through either their private life or through work. This can include feelings of guilt and self-blame. Friends and colleagues of those found to have committed fraud can also be impacted.

1.4 Types of fraud

- Fraud is nothing new but over time it has become increasingly sophisticated as technology has improved. The development of artificial intelligence (AI) will bring further risks.
- Fraudsters use a whole range of methods to trick their victims and evolve their tactics over time. They can also pressure their targeted victims into making quick decisions, potentially overriding controls in place. Vigilance is important to prevention. Even something claiming to support fraud prevention might be a fraud itself.

Some of the most regularly used methods that are relevant to the education sector include the following:

External:
External fraud is where parties outside of an organisation target an organisation illegally for some kind of financial benefit, examples below:

- Cyber fraud
- Phishing (electronic impersonation)
- Malware
- Artificial intelligence (AI)
- Invoice fraud
- Certificate fraud or qualification fraud
- Banking fraud
- Money laundering

- Procurement fraud

Internal:
Internal fraud is when an employee or employees commit (or attempt to commit) a fraud against the organisation they work for. These can be hard to detect, as employees have inside knowledge of systems and processes the organisation uses and are aware of system weaknesses and vulnerabilities.

Internal fraud can include:
- falsified travel expenses
- theft of assets
- accepting inappropriate gifts and hospitality
- plots to transfer money out of the organisation
- theft of cash
- non-receipt of income
- substitution of personal cheques for cash
- travelling and subsistence claims for non-existent journeys/events
- travelling and subsistence claims inflated
- manipulating documentation to increase salaries/wages received, e.g. false overtime claims
- payment of invoices for goods received by an individual rather than the individual Academy
- failure to observe, or breaches of, regulations and/or other associated legislation laid down by the Trust
- breaches of confidentiality regarding information
- creation of false documents
- deception
- using position for personal reward
- collusion from unknown and undeclared interests and relationships.

The above list is not intended to be definitive, fraud can take many different paths. If in any doubt about whether a matter is an irregularity or not, clarification must be sought from the Trust Director of Finance or Chief Operating Officer. Our Financial Regulations provides for controls to minimise the risk of the above occurring.

Fraud personas
Fraud personas (initially developed by the Commonwealth Fraud Prevention Centre) are linked to the way somebody is contributing to a fraud and help us understand the kind of behaviours that a fraudster might display. Personas include:

- a corruptor – who abuses their position of entrusted power
- a deceiver – who makes others believe something to be true which isn't
- an enabler – who allows a fraud they know about to happen
- an exploiter – who uses information they are aware of to make dishonest gain
- a fabricator – who invents or produces false documents and information
- an impersonator – who pretends to be somebody else to make personal gain
- an organised group – who work in a co-ordinated way to make dishonest gain

1.5 Preventing Fraud

- Fraud and corruption can negatively impact our reputation and result in financial loss of scarce funds given to us to deliver exceptional education. Fraud can be time consuming to investigate and identify and will likely be disruptive and unsettling to all involved. Preventing fraud is paramount. Establishing and maintaining a suitably robust internal control framework will reduce the opportunity for fraud to take place and give business leaders appropriate

assurances that we take fraud seriously and have taken steps to minimise the chances of a fraud occurring and limiting its impact if it does.

- Wherever possible, appropriate levels of authorisation and segregation of duties are embedded within and systems and procedures.
- Fraud can be minimised through carefully designed and consistently operated procedures which deny opportunities for fraud. Staff are made aware of policies through the induction programme and notification of policy updates through the staff Intranet.
- Staff recruitment procedures require applicants to declare any connections with Members, Trustees, Academy LGB Governors and existing Trust staff. Likewise, it is incumbent Members, Trustees, LGB Governors and existing staff that make up a selection panel to declare any connection to any applicant.
- The IT Services Manager will ensure that systems are protected by controls that comply with legislation and the requirements laid down by the Department for Education (DfE).
- Our Financial Regulations help to ensure that financial management is always conducted in accordance with the highest standards.
- This policy is published on our website. Members, Trustees, LGB Governors and staff are made aware of our expectations through robust induction procedures and regular training. This policy can also be found on our Smartlog portal.

1.6 Detection

- We cannot give absolute assurance that all fraud can be prevented. We have established policies, procedures and system-based controls in place to detect and highlight irregular transactions. We expect senior staff and their managers to actively promote compliance with our systems and procedures. All staff are expected to speak-up if they have concerns about an individual, group of individuals, the appropriateness of a particular transaction, contract, relationship or anything that may constitute fraudulent activity. Please see our Whistleblowing policy for more guidance on this subject.
- We have established systems and procedures in place, including detail financial regulations and controls related to cyber-crime, all forming part of our internal control framework.

2 Fraud Response Plan

This plan also applies to cyber-enabled frauds and cyber incidents (for example ransomware, phishing, or supplier mandate fraud). Please see our Cyber Critical Incident plan for more details.

2.1 Purpose

The purpose of this plan is to define authority levels, responsibilities for action and reporting lines in the event of a suspected fraud or financial irregularity. The use of the plan should allow us to:

- respond quickly and professionally to any suspicion or suggestion of fraud or irregularity
- prevent further loss
- establish and secure evidence necessary for criminal or disciplinary action
- assign responsibility for investigating the incident
- establish circumstances in which external specialists should be involved
- establish circumstances in which the police should be notified and establish lines of communication with the police
- notify the DfE, in accordance with the Academy Trust Handbook. The current threshold for reporting is more than £5,000, individually or cumulatively, within any financial year.
- minimise and recover losses
- take appropriate action against those who have committed the fraud
- deal with requests for references for employees disciplined or prosecuted for fraud
- review the reasons for the incident, the measures taken to prevent a recurrence, and any action needed to strengthen future responses to fraud
- Maintain appropriate communication channels with all ‘need to know’ persons

2.2 Initiating Action

- All actual or suspected incidents should be reported immediately. We will treat all reported cases seriously.

- If the fraud relates to a breach of financial regulations, where the Director of Finance is not the perpetrator (or assumed perpetrator), the fraud should be reported to the Director of Finance.
- If the disclosure involves or implicates the CEO, COO, Director of Finance or Head Teacher/Principal, then the disclosure should be made to the Chair of Trustees via the Trust Governance Professional. If the Trust Governance professional has the potential to be implicated, The Trust Chair should be contacted through the CEO. If the Trust Chair has the potential to be implicated, the Trust Governance Professional should be made aware and will determine what steps to take, depending on the nature of the alleged fraud and persons involved.
- To ensure that any further investigation, including criminal investigation, are not compromised it is important that you do not discuss the disclosure with anyone else.
- As soon as practicable, ideally within 24 hours, a 'Fraud Review and Response Group (FRRG)' meeting should be convened normally consisting of the following group to decide on the initial response:
    - Director of Finance
    - CEO
    - COO
    - The Trust Governance Professional if the alleged fraud involves a Trust member, Trustee, senior staff member or Local Governing Body Governor.
- Should it be necessary, the FRRG will appoint a suitably experienced officer to undertake an investigation, supported by HR colleagues and the Trust Internal Audit Service provider as appropriate.
- In the case of cyber-enabled frauds and cyber incidents, the Director of IT and Facilities will be immediately notified and will respond in line with the cyber incident response plan.
- The Chair of the Audit and Risk Committee and Chair of Trustees should be advised at the earliest possible time that an investigation is taking place.

2.3 Prevention of further loss

- Where initial investigation provides reasonable grounds for suspecting a fraud has taken, or is taking, place, the FRRG will decide what steps need to be taken to prevent further loss. This may require the suspension of the individual(s) suspected of fraud. It may be necessary to plan the timing of suspensions to prevent individuals from destroying or removing evidence that may be needed to support the investigatory process
- Suspension will be in accordance with college disciplinary procedures.
- Through the Director of IT and Facilities, access to Trust buildings and IT systems will be suspended with immediate effect for all persons potentially implicated in the fraudulent activity. If the potential fraud includes the Director of IT and Facilities, instruction will be given to a member of the Trust IT Team where it is reasonable to assume that they are not connected.
- The investigatory officer and/or Internal Audit Service Provider shall consider whether it is necessary to investigate systems other than that which has given rise to suspicion, through which the individuals/respondents may have had the opportunity to perpetrate the fraud.
- If the nature of the fraud and value (both economic and reputational) are sufficiently material (£5,000 being the threshold), the investigating officer should seek legal advice to establish whether or not any furth investigation should be conducted by an external investigator or be passed to the Police.

2.4 Establishing and securing evidence

- We will follow our disciplinary procedures against any member of staff who has committed fraud and pursue the prosecution of any such individual.
- Those investigating the incident will:
    - maintain familiarity with our disciplinary procedures and ensure that evidence requirements will be met during any fraud investigation
    - obtain approval from the CEO/COO or Chair of Trustees if appropriate prior to establishing and maintaining contact with the police
    - ensure that staff involved in fraud investigations are familiar with and follow rules on the admissibility of documentary and other evidence in criminal proceedings

- Please see section 4 for more detail on what to do and what not to do should you suspect a fraud is being perpetrated.

2.5 Notification to DfE

- The circumstances in which we must inform DfE about actual or suspected frauds are detailed in the Academy Trust Handbook.
- We are required to report all material fraud or irregularity to the DfE where one or more of the following apply:
    - The sums involved are or are potentially more than £5,000
    - The particulars of the fraud or irregularity are novel, unusual, systematic, or complex
    - There is likely to be public interest because of the nature of the fraud or irregularity, or the people involved.
- There may be cases of fraud or other impropriety or irregularity which fall outside the above criteria, we will seek advice or clarification from the DfE if appropriate.
- The Director of Finance is responsible for informing DfE of any such incidents and will confirm to the Accounting Officer that a report has been made. The Chair of the Audit and Risk Committee will also be informed of the report.

2.6 Notification to External bodies

- Fraud, including any suspected or attempted fraud, should be reported to Action Fraud to help identify systematic risks potentially affecting whole sectors (for example cybercrime). Action Fraud monitors the cost of fraud across the UK and has been set up to provide a single point of reporting and information for individuals and organisations.
- In addition, significant cyber incidents (e.g., data breaches or ransomware) will also be reported to the Information Commissioner's Office (ICO) as well as the DfE where applicable. Cyber incidents should be documented in accordance with our Cyber Incident Response Playbook. We will inform the Trust/academy insurer.

2.7 Recovery of Losses

- Recovering losses is a major objective of any fraud response investigation. Those investigating the incident should ensure that in all fraud investigations the amount of any loss is quantified. Repayment of losses will be sought in all cases.
- Where the loss is substantial, legal advice should be obtained without delay to establish the most appropriate way forward that maximises our prospects of recovery. Where a civil action is taken against a perpetrator, we will always seek to recover our legal costs on top of losses arising from the fraudulent act.
- We will seek advice from our insurers on potential loss recovery where the value exceeds £5,000.

2.8 References for employees disciplined or prosecuted for fraud

- It is a requirement that any request for a reference for a member of staff who has been disciplined or prosecuted for fraud shall be referred to Human Resources. Human Resources shall prepare any answer to a request for a reference having regard for employment law.

2.9 Reporting arrangements

- Where an event gives rise to suspicion of fraud it must be reported without delay to the Accounting Officer (CEO), the Chair of Board, and the Chair of the Audit Committee. These reporting arrangements may need to be varied if any of the individuals are implicated, potentially or otherwise, in the act itself.
- Any variation from the approved fraud response plan, together with reasons for the variation, shall be reported promptly to the Chair of Board and the Chair of the Audit and Risk Committee.
- On completion of the investigation the FRRG will submit to the Audit and Risk Committee, and the DfE is required to do so, a report containing:
    - a description of the incident, including the value of any loss, the people involved and the means of perpetrating the fraud
    - Routes to recovery of losses and the likelihood of recovery

- What disciplinary action is/has being taken
- Progress with any criminal investigation if taken forward
- the measures taken to prevent recurrence
- any action needed to strengthen future responses to fraud with follow up report on whether the actions have been taken
- estimate of resources required to conclude the investigation

2.10 Responsibility for investigation

- The Director of Finance shall normally lead all investigations
- Some investigations may require the use of specialists or technical expertise. Where a case is not pursued by the Police, in these circumstances the FRRG group may approve the appointment of external specialists to lead or contribute to the special investigation. If the Police pursue Criminal Proceedings, we will be guided by them on how to best conclude our investigation.

2.11 Review of fraud response plan

- This plan will be reviewed for fitness of purpose bi-annually or after each use. Future changes to this policy will be submitted to the Audit and Risk Committee for recommendation to the Board of Trustees for approval.
- The management of Cyber related Fraud is covered within our Cyber Incident Response Plan; this policy will be used in conjunction with that plan to determine arrangements for dealing with any fraud arising from a Cyber related incident.

3 Additional Guidance

3.1 Indicators of Fraud (taken from the DfE guidance Indicators for potential fraud: a generic checklist for educational providers)

Introduction

This is a generic list of red flags that could indicate fraudulent activity in your organisation, including bribery and corruption.
We've categorised them into:

- personal motives for fraud
- organisational motives for fraud
- weaknesses in internal controls
- transactional indicators
- possible methods used to commit or conceal fraud
- recordkeeping, banking and other

Due to the nature of fraud, red flags may not be exclusive to just one area.

This document is not exhaustive and is a guide only. It may be helpful as a checklist if you have concerns that fraudulent activity might be taking place.

Not all indicators may be relevant to all organisations.

3.2 Personal motives for fraud

Consider if any of these red flags are present in your organisation.

1. Do personnel believe they receive inadequate compensation and rewards (such as recognition, job security, annual leave or promotion)?
2. Does anyone have evidence of an expensive lifestyle (such as cars or trips) that seems disproportionate to their income?
3. Is anyone experiencing personal problems (such as with gambling, alcohol, drugs or debt)?
4. Is there an unusually high degree of competition or peer pressure?

5. Are there related-party transactions (business activities with personal friends, relatives or their companies)?
6. Are there any unrecorded or unmanaged conflicts of interest?
7. Are there any disgruntled employees (such as those who have recently been demoted or reprimanded)?
8. Has there been a recent failure associated with a specific individual?
9. Is there any personal animosity or professional jealousy?

3.3 Organisational motives for fraud

Consider if any of these red flags are present in your organisation.

1. Is the organisation experiencing financial difficulty?
2. Is the commercial arm experiencing financial difficulty?
3. Are deadlines to achieve outputs particularly tight?
4. Does the organisational governance lack clarity, direction or substance?
5. Is the organisation closely identified with or dominated by one individual?
6. Is the organisation under pressure to show results (such as budgetary matters or exam results)?
7. Has the organisation recently suffered disappointment or negative consequences as the result of bad decisions?
8. Does the organisation want to expand its scope or obtain additional funding?
9. Are funding awards or contracts for services up for renewal or continuation?
10. Is the organisation due for a site visit by auditors, Ofsted or others?
11. Does the organisation have a for-profit component?
12. Has the organisation recently been affected by new or changing conditions (such as regulatory, economic or environmental)?
13. Is the organisation facing pressure to use or lose funds to sustain future funding levels?
14. Is there a record of previous failures by one or more organisational areas, associated businesses or key personnel?
15. Have there been sudden changes in organisational practice or the usual pattern of behaviour?

3.4 Weaknesses in internal controls

Consider if any of these red flags are present in your organisation.

1. Is there a general lack of transparency about how the organisation works and implements procedures and controls?
2. Does management demonstrate a lack of:
    - attention to ethical values, including a lack of communication regarding the importance of integrity and ethics?
    - concern about the presence of temptations and inducements to commit fraud?
    - concern regarding instances of fraud?
3. Is there a clear fraud response plan or investigation policy?

4. Does management fail to specify or require appropriate levels of qualification, experience or competence for employees?

5. Does management display a tendency to take risks?

6. Is there a lack of appropriate organisational and governance structure, with defined lines of authority and reporting responsibilities?

7. Does the organisation lack policies and communication relating to individual accountability and best practice (for example, related to procurement, travel and subsistence, use of alcohol, or declarations of interest)?

8. Is there a lack of human resources policies and recruitment practices?

9. Does the organisation lack employee performance appraisal measures or practices?

10. Does management display a lack of commitment towards the identification and management of risks relevant to the preparation of financial statements (that is, they do not consider the significance of risks, the likelihood of occurrence or how they should be managed)?

11. Is there inadequate comparison of budgets with actual performance and costs, forecasts and prior performance? Is there no regular reconciliation of control records and a lack of proper reporting to a governing body?

12. Is the management of information systems inadequate (such as having no policy on information technology security, computer use and access, verification of data accuracy, or completeness or authorisation of transactions)?

13. Is there insufficient physical security over facilities, assets, records, computers, data files and cash? Is there a failure to compare existing assets with related records at reasonable intervals?

14. Is there inadequate or inappropriate segregation of duties regarding initiation, authorisation and recording of transactions, maintaining custody of assets and the like?
15. Are accounting systems inadequate (that is, there is an ineffective method for identifying and recording transactions, no tracking of time periods during which transactions occur, insufficient descriptions of transactions and 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 prevent missing payment dates)?

16. Are the purchasing systems and procedures inadequate (such as poor or incomplete documentation to support procurement, purchase, payment or receipt of goods and services, and poor internal controls for authorisation and segregation of duties)?

17. Do subcontractor records and systems reflect inadequate internal controls?

18. Is there a lack of internal, ongoing monitoring of the controls that are in place or failure to take any corrective actions, if needed?

19. Is management unaware of, or does it display a lack of concern about applicable laws and regulations (for example, companies acts, charities acts, child protection, funding agreement, contract for services)?

20. Are there specific problems or reportable conditions that were identified by prior audits or other means of oversight that have not been corrected (such as a history of problems, a slow response to past findings or problems, or unresolved present findings)?

21. Is there no mechanism to inform management, directors, trustees or governors of possible fraud?

22. Is there a general lack of management oversight?

3.5 Transactional indicators

Consider if any of these red flags are present in your organisation.

1. Are there related-party transactions with inadequate, inaccurate or incomplete documentation or internal controls (such as business or research activities with friends, family members or their companies)?

2. Does the not-for-profit entity have a for-profit counterpart with linked infrastructure (such as a shared board of trustees, governors or other shared functions and personnel)?

3. Are there specific transactions that typically receive minimal oversight?

4. Are there previous audits with findings of:
    - questioned costs?
    - evidence of non-compliance with applicable laws or regulations?
    - weak internal controls?
    - a qualified audit opinion?
    - inadequate management response to any of the above?

5. Are transactions or accounts difficult to audit or subject to management judgement and estimates?

6. Are there multiple sources of funding with inadequate, incomplete or poor tracking, failure to segregate funds or the existence of pooled funds?

7. Are there unusual, complex or new transactions, particularly if they occur at year end, or the end of a reporting period?

8. Are there transactions and accounts operating under time constraints?

9. Are there travel accounts with inadequate, inaccurate or incomplete documentation or poor internal controls such as:
    - appropriate authorisation and review?
    - 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?

10. Are there credit card accounts with inadequate, inaccurate or incomplete documentation or internal controls (such as appropriate authorisation and review)?

11. Are there accounts in which activities, transactions or events involve handling of cash or wire transfers, or are there high cash deposits maintained with banks?

12. Are there assets that are easily converted to cash, such as items that are:
    - small size, high value, high marketability or lack of ownership identification?
    - easily diverted to personal use, such as cars, houses, equestrian centres or villas?

13. Are there accounts with large or frequent shifting of budgeted costs from one cost centre to another without adequate justification?

14. Does the payroll (including fringe benefits) system have inadequate controls to prevent an individual being:

- paid twice?
- paid for non-delivery or non-existence?
- outsourced but with poor oversight of starters, leavers and payments?

15. Are consultant agreements vague about work carried out, the time period covered, the rate of pay or the product expected, or is there a lack of proof that the product or service has actually been delivered?

16. Are sub-contractor agreements vague about work carried out, the time period covered, the rate of pay or the product expected, or is there a lack of proof that the product or service has actually been delivered?

17. Is there a sudden or rapid growth of newly contracted or existing education providers, for example:
    - a rapid or significant increase in learner numbers for newly contracted providers?
    - providers with large cohorts of newly recruited learners in occupational areas where the provider has minimal or no previous experience?
    - concerns that a provider's infrastructure or staffing is insufficient to manage the increase in learners?

3.6 Methods used to commit or conceal fraud

Consider if any of these red flags are present in your organisation.

1. Are there employee indicators such as:
    - an eagerness to work unusual hours?
    - access to or use of computers at unusual hours?
    - a reluctance to take leave or seek support?
    - an insistence on doing tasks alone?
    - the refusal of a promotion or a reluctance to change job?

2. Are there employee issues with auditors such as:
    - a 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 the auditors?
    - an attempt to control the audit process (such as its timetables, access or scope)?
    - the auditee or employee blaming a mistake on a lack of experience with financial requirements or regulations governing funding
    - promises of co-operation followed by subsequent excuses to limit or truncate co-operation?
    - subtle resistance?
    - answering a question that was not asked?
    - offering more information than was asked for?
    - providing a wealth of information in some areas but little in others?
    - explaining a problem by saying, "We've always done it that way" or "Someone at DfE [or elsewhere] told us to do it that way" or "Mr X said he'd take care of it"?
    - a tendency to avoid personal responsibility (indicated by the overuse of "we" and "our" rather than "I")?
    - blaming someone else?
    - too much forgetfulness?
    - trying to rush the audit process?
    - an uncharacteristic willingness to settle questioned costs in an attempt to deter further investigation or analysis?

3. Is there a general lack of transparency about how the organisation works, and about its procedures and controls?

4. Are explanations fabricated to support an inability or unwillingness to provide evidence for transactions or assets (such as stated computer failure, loss of electronic data or theft of business records or assets)?

3.7 Recordkeeping, banking and other red flags

Consider if any of these red flags are present in your organisation.

1. Are documents missing, copies rather than originals, in pencil or altered, or do they contain false signatures, the signature of an incorrect person or no authorisation where it would be expected?
2. Is there deviation from standard procedures (for example, all files but one having been handled a particular way or all documents but one having been included in a file)?
3. Are there excessive or poorly evidenced journal entries, or a lack of explanation for journal entries?
4. Are there transfers to or from any type of holding or suspension account?
5. Are there inter-fund company loans to other linked organisations?
6. Are there records that are inadequate or have not been updated or reconciled?
7. Are several different banks or bank accounts being used, or have there been frequent changes of bank?
8. Has there been a failure to disclose unusual accounting practices or transactions?
9. Are there unusual accounting practices or transactions, such as:
    - an uncharacteristic willingness to settle questioned costs?
    - non-serial-numbered transactions or out-of-sequence invoices or other documents?
    - the creation of fictitious accounts, transactions, employees or charges?
    - the writing of large cheques to cash or repeatedly for a particular individual?
    - excessive or large cash transactions?
    - payroll checks with unusual or questionable endorsements?
    - payees who have similar names or addresses?
    - non-payroll checks written to an employee?
10. Have delivery needs been defined in ways that can only be met by one source or individual?
11. Is there continued reliance on a person or entity despite poor performance?
12. Have non-business or personal goods or services been treated as business transactions in financial records (such as goods and services purchased for trustees, directors or their family members)?
13. Has the directors' loan account facility been misused (for example, deliberately miscoding transactions to gain personal advantage)?
14. Are material goods or services fictitiously or erroneously reported as having been purchased, with evidence fabricated to support the claim, so they can be used as a conduit to remove funds from the organisation? Potential evidence could include:
    - repeated purchases of the same items
    - identical items purchased in different quantities within a short time period
    - invoices and statements used as evidence for purchases facilitating duplicate transactions or payments
    - anomalies in the format of purchase invoices
    - goods and equipment not being used as promised, or that do not work or do not exist
15. Are legitimate business assets being used for non-business or private use?

3.8 Examples and Indicators of Cyber Fraud

Cyber fraud often takes the form of phishing and impersonation attacks.

Common Examples:

- **Phishing Emails/Messages:** Scammers send messages that look authentic (e.g., from a bank, a senior manager, or an energy provider) to trick victims into revealing sensitive information, clicking a malicious link, or making a fraudulent payment.
- **Malware Distribution:** Fraudsters may send an invoice with an attachment that, when opened, installs malicious software on your computer without your knowledge.
- **Fake Websites/Profiles:** Criminals create fake websites or social media profiles that look like a real organisations to steal donations or personal information.
- **Business Email Compromise (BEC):** Emails that appear to come from a high-ranking person (e.g., CEO, manager) urgently requesting a payment to a specific bank account.
- **Account Hacking:** Gaining access to email or social media accounts to extort the victim or scam their contacts.
- **Indicators of Fraudulent Attempts:**
- **Poor Spelling and Grammar:** While scams are getting smarter, many still contain obvious spelling, grammar, or punctuation errors.
- **Generic Greetings:** The message uses a general greeting like "valued customer" instead of your name.
- **Sense of Urgency or Threat:** The message pressures you to act quickly (e.g., "send these details within 24 hours" or "act immediately").
- **Suspicious Sender Details:** The sender's name or email address looks slightly off, or the design/quality is not what you would expect from a credible organisation.
- **Unexpected Requests:** Any unsolicited message asking for personal details, passwords, or a payment to a new bank account should be treated with suspicion.
- **Suspicious Links/Attachments:** The message includes a link to a website with a strange address, or an unexpected attachment.

3.9 Methods used to commit and/or conceal fraud

- Employee indicators such as eagerness to work unusual hours, access to/use of computers at unusual hours, reluctance to take leave/seek support, insistence on doing job alone and/or refusal of promotion or reluctance to change job
- Auditor/employee issues such as:
- refusal or reluctance to provide information/turn over documents
- unreasonable explanations
- annoyance/aggressive responses to at questions/requests in an attempt deter auditors
- trying to control the audit process (timetables, access, scope)
- auditee/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 co-operation
- subtle resistance
- answering a question that wasn’t asked
- offering more information than asked
- providing wealth of information in some areas, little to none in others
- explaining a problem by saying “we’ve always done it that way”, or “someone at DfE (or elsewhere) told us to do it that way” or “Mr X said he’d take care of it”; a tendency to avoid personal responsibility (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/analysis
- A general lack of transparency about how the organisation works, procedures and controls
- Fabricated explanations to support inability or unwillingness to evidence transactions/assets (such as stated computer failure/loss of electronic data, or stated theft of business records/assets).

3.10 Record keeping/banking/other

- Documents:
    - missing documents
    - documents are copies, not originals

    - documents in pencil; altered documents
    - false signatures/incorrect person signing/no authorisation where it would be expected
- Deviation from standard procedures (for example, all files but one managed a particular way; or all documents but one included in file)
- Excessive and/or poorly evidenced journal entries, unable to provide explanations for journal entries
- Transfers 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 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, such as: uncharacteristic willingness to settle questioned costs; non-serial-numbered transactions or out-of-sequence invoices or other documents; creation of fictitious accounts, transactions, employees, charges; writing large cheques to cash or repeatedly to a particular individual; excessive or large cash transactions; payroll checks with unusual/questionable endorsements; payees have similar names/addresses; and/or non-payroll checks written to an employee
- Defining delivery needs in ways that can only be met by one source/individual
- Continued reliance on person/entity despite poor performance
- Treating non-business and/or personal goods or services as business transactions in financial records (such as goods and services purchased by Members, Trustees, governors, directors, and/or their family members)
- Materials goods and/or services fictitiously erroneously reported as purchased; evidence fabricated to support claim, can be used as conduit to remove funds from organisation. Potentially evidenced by:
    - repeated purchases of same items;
    - identical items purchased in different quantities within a short time period;
    - invoices and statements used to evidence purchase facilitating duplicate transactions/payments;
    - anomalies in format of purchase invoices;
    - and/or goods/equipment not used as promised, doesn't work, doesn't exist
    - Legitimate business assets put to non-business/private use

4 What to do and not to do if you suspect fraudulent activity

In addition to the warning signs detailed previously, staff and students are advised to take notice of the following "Dos and Don'ts" in respect of possible fraud-related instances or actions:

DO:

Report your suspicions as soon as you feel appropriate
It is not your responsibility to undertake a comprehensive investigation so please do not wait as this may give the fraudster the opportunity to cover their tracks.

Make a record of your concerns without delay, include:

- The nature of your concern(s)
- Who you believe is/are potentially involved
- Details of any conversations you might have had, please include the date and time and if you have any witness(es)
- Please provide dates and times for any event you believe is relevant
- Remember to sign and date your note

Keep any evidence you have, this could be:

- Emails, text messages, screen shots, written notes

- Records of any conversations
- Physical proof (letters, printed documents etc)

DON'T:

Be afraid to speak up.
The Public Interest Disclosure Act provides protection for all employees who raise a reasonably held concern via the proper channels. We have a separate Whistleblowing policy that gives more detail. If you follow our procedures you will not suffer any discrimination, we will always treat every reported case with the utmost sensitivity and confidentiality.

Discuss your concerns with anyone other than the nominated Officer for Richard Huish Trust, the Director of Finance.
We will thoroughly investigate all reported concerns. It could be that there is a reasonable explanation for the events that gave rise to your concerns, it is important that we do not jump to conclusions prior to the completion of a thorough investigation being concluded, just as we want to hold individuals to account for any fraudulent actions we would also wish to protect them if our investigation concludes that there is no case to answer.

If your concerns pertain to the Director of Finance, please make your concerns know to the Trust CEO or the Trust Governance Professional if more appropriate.

Undertake your own investigation or confront the person(s) you suspect.
There are special rules that govern how evidence must be gathered that could lead to a criminal case, we would want to make sure that staff that have received appropriate training and understand these special rules conduct any investigation. They will also know when best to inform the police and other bodies.

5 Anti- Fraud Checklist

Sadly, educational institutions are not immune from fraud. The ten questions below are intended to help provide a framework within which we can test our arrangements for preventing, detecting, and dealing with fraud should it occur.

1. Are Members, Trustees, LGB Governors, the Accounting Officer and other senior staff aware of the risk of fraud and their responsibilities about fraud?
2. Do we regularly review our counter fraud strategy, fraud risk assessment processes, and fraud response plan?
3. Have we established systems and processes to respond quickly and effectively into allegations of suspected fraud, and responding to actual fraud when it arises?
4. Do we engender an anti-fraud culture throughout our Trust, for example, do we have:
5. a clear statement of commitment to ethical behaviour?
6. a clear focus on prevention?
7. sound financial regulations (including segregation of duties)?
8. sound recruitment and induction processes?
9. robust disciplinary procedures?
10. Is fraud risk included within the remit of our Audit and Risk Committee Terms of Reference?
11. Is fraud risk considered within our risk management process?
12. Do we regularly review policies on whistleblowing, declarations of interest and receipt of gifts and hospitality?
13. Is it clear how and to whom suspicions of fraud in our Trust should be reported, both internally and externally (e.g. Action Fraud, external auditors, regulators, DfE as necessary)?
14. Do we evaluate the effectiveness of anti-fraud measures in reducing fraud?
15. Do we undertake 'lessons learned' exercises when suspected or actual fraud has taken place?

6 Useful resources

There are a wide range of materials and resources available relating to counter-fraud and fraud awareness both within the education sector and beyond.

The following resources are intended to be helpful as reference points.

- Cyber security training for school staff
- Cyber security breaches survey 2024: Educational Institutions
- Government Counter Fraud Functional Strategy 2024 to 2027
- Tackling qualification fraud
- How to report serious incidents in your charity
- Protect your charity from cyber-crime
- Protect your charity from fraud
- National Fraud Initiative
- Tackling fraud and corruption against government
- Cyber security blog
- Code of practice on managing the risk of fraud and corruption
- Stop Think Fraud
- Action Fraud
- National Cyber Security Centre
- National Crime Agency – fraud section
- Public Sector Fraud Authority
- Local Government Association Counter Fraud Hub
- Protect
- Academies Finance Professionals Power Hour – presentation on counter-fraud by DfE