

Anti-Fraud Policy and Response Plan

Policy number:	FI010	Policy Owner:	Executive Director, Finance
EIA Status:	Compliant	EIA meeting date:	[EIA Meeting Date]
Approved by:	SLT	Date approved:	November 2025
	Committee		November 2025
	Board		n/a
Review frequency:	Annually	Next review due:	02/11/2026
External website:	Yes	Status:	Active
Linked policies/ documents	<ul style="list-style-type: none"> • Codes of Conduct (including Anti-Bribery requirements) • Financial Regulations Policies on gifts and hospitality, claiming of expenses • Sound internal control systems Effective internal audit • Effective recruitment and selection procedures • Disciplinary procedure • Whistleblowing (Public Interest Disclosure) Policy • Register of Interests • Training Procedures for enrolment of students 		

Anti-Fraud Policy and Response Plan

1. Policy Statement and Purpose

Introduction

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

- The College is committed to protecting the public funds with which it has been entrusted. It is essential that losses due to fraud and corruption are minimised in order to ensure resources are used for their intended purpose of providing education
- The public is entitled to expect the College to conduct its affairs with integrity, honesty and openness and demand the highest standards of conduct from both staff and students. This Anti-Fraud Policy outlines its commitment to creating an anti-fraud culture and maintaining high ethical standards in its administration of public funds
- The Policy is based on best practice models within the education sector. The Policy is also based on a series of comprehensive and inter-related policies and procedures that provide a corporate framework to counter fraudulent activity. These have been formulated in line with appropriate legislative requirements, and include:
 - Codes of Conduct (including Anti-Bribery requirements)
 - Financial Regulations
 - Policies on gifts and hospitality, claiming of expenses
 - Sound internal control systems
 - Effective internal audit
 - Effective recruitment and selection procedures
 - Disciplinary procedure
 - Whistleblowing (Public Interest Disclosure) Policy
 - Register of Interests
 - Training
 - Procedures for enrolment of students

Culture

- The College believes 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 its commitment to maintaining the highest standards of governance, the College has defined acceptable behaviour which both staff and students are expected to follow. These are based on the Nolan Principles of Standards in Public Life.
- The staff and students at the College 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 College business or activity.

Definitions of Fraud

- The Fraud Act 2006 defines fraud as a criminal offense involving deception with the intent to gain an advantage or cause loss to another person. It encompasses three main types of fraudulent activities:
 - **Fraud by false representation:** Deceiving someone by presenting false information.
 - **Fraud by failing to disclose information:** Not revealing important information that would affect a decision.
 - **Fraud by abuse of position:** Misusing a position of trust to gain an advantage.Fraud also includes cyber-enabled activities such as phishing, ransomware, malware attacks, invoice or mandate fraud, impersonation (including AI-generated or deepfake communications), and other cybercrime intended to obtain money, data, or unauthorised access to systems
- Fraud can occur anywhere within the College and can present itself not simply as financial or financially motivated but covers areas including financial, reputational, employment and students. This Policy covers all the above
- For practical purposes of the application of this policy, fraud may be defined as the use of deception with the intention of:
 - gaining an advantage, personally and for family or friends; or
 - avoiding an obligation; or
 - causing a financial loss to the College.
- The main types of irregularity are:
 - Theft – this may include the removal or misuse of funds, assets, or cash
 - False accounting – dishonestly destroying, defacing, concealing, or falsifying any account, record or document required for any accounting purpose, with a view to personal gain or gain for another, or with the intent to cause loss to the College or furnishing information, which is or may be misleading, false, or deceptive
 - Abuse of position – abusing authorities and misusing College resources or information for personal gain or causing loss to the College. advantage, personally and for family or friends; or
 - Avoiding

Common examples of Education fraud are provided at Section C Additional Guidance of this document.

The College's Financial Regulations provides for controls to minimise the risk of the above occurring.

Prevention

- Fraud and corruption are costly, both in terms of reputational risk and financial losses, as well as time-consuming to identify and investigate, disruptive and unpleasant. The prevention of fraud is therefore a key objective. Measures should be put in place to deny opportunity, provide effective leadership, auditing, employee screening, and student recruitment
- 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 existing Members of the Corporation Board and staff. Members of staff recruitment panels are similarly required to declare such connections.
- The IT Services Manager will ensure that systems are protected by controls including multi-factor authentication, timely patching, regular backup testing, and phishing simulation exercises
- The College's Financial Regulations help to ensure that at all times the financial management of the College is conducted in accordance with the highest standards. Continuous management review of systems, and reports by internal audit should assist in preventing and detecting fraud; and should also result in system improvements. The risk of fraud should be a factor for consideration in audit plans.
- Key determinants of the standards of behaviour in an organisation will be the standards observed by governing bodies and senior managers; and the policies and approach to their enforcement promoted from the top.
- The credibility and success of the Anti-Fraud Policy is dependent largely on how effectively it is communicated throughout the organisation. The Policy is published on the College's website and is available on the staff Intranet.
- The Senior Leadership Team should review the Post 16 Audit Code of Practice Anti-Fraud checklist on an annual basis. Please refer to the checklist in Annex C Additional Guidance which sets out the following framework:
 - a fraud risk assessment to identify areas most vulnerable to suspected fraud; DfE has developed a list of potential fraud indicators to support a review (refer to Annex C)
 - testing of internal control systems to ensure robustness and to help assess vulnerability to fraud
 - policies and procedures in place (such as a whistleblowing policy and a fraud response plan), detailing how to report suspected fraud and the processes to follow when reports are received
 - an exercise to evaluate the scale of suspected fraud
 - a means of measuring the effectiveness of the counter fraud strategy

Detection

- No system of preventative measures can guarantee that fraud will not occur. However, policies and procedures are in place to detect and highlight irregular transactions. It is the responsibility of senior officers and their managers to prevent and detect fraud by maintaining good control systems within their departments and making sure that all staff understand the systems and work within them
- The College has established systems and procedures in place which incorporate effective and efficient internal controls. The College has published Financial Regulations which require employees to follow standard practices when conducting the College's affairs, to act in accordance with best practice and adhere to agreed internal control systems
- Automated monitoring and alerting will be implemented to detect cyber-enabled fraud attempts, such as phishing or unauthorised access attempts. Logs of financial and

administrative systems are retained for forensic review, if needed, through the College's backup protocols.

- The College has a Whistleblowing Policy. The policy is reviewed regularly
- Robust preventative measures by management, coupled with sound checks and balances, are adopted by the College.

2. Fraud Response Plan

This plan also applies to cyber-enabled frauds and cyber incidents (for example ransomware, phishing, or supplier mandate fraud).

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 the College 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 DfE, in accordance with the Post 16 Audit Code of Practice. The current threshold for reporting is frauds in excess of £10,000
- 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
- keep all persons with a need to know suitably informed about the incident and the College's response

Initiating Action

- Suspicion of fraud or financial irregularity may be captured through a number of means, including the following:
 - requirements on all staff under the Financial Regulations to report fraud
 - Public Interest Disclosure Policy otherwise known as "Whistleblowing"
 - planned audit work

- operation of proper management control and procedures
- All actual or suspected incidents should be reported immediately either: :
 - requirements in accordance with the Financial Regulations to the Director of Finance, or
- If the disclosure involves or implicates any of the individuals detailed above, then the disclosure should be made to the Chair of the College Board
- As soon as practicable, ideally within 24 hours, a meeting should be convened normally consisting of the following group to decide on the initial response:
 - Director of Finance
 - Principal/Chief Executive

At some stage it may also be necessary to involve Student Services and Marketing if there are potential public relations/media issues.

- In the case of cyber-enabled frauds and cyber incidents, the IT Services Manager will be immediately notified and will coordinate with senior management and external cyber incident response providers as appropriate. involves or implicates any of the individuals detailed above, then the disclosure should be made to the Chair of the College Boar
- The Chair of the Audit Committee should be advised at the earliest possible time that an investigation is taking place.

Prevention of further loss

- Where initial investigation provides reasonable grounds for suspecting a member/ member of staff of fraud, the project group will decide how 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.
- Vice Principal Central Services should advise on the best method of denying access, while individuals remain suspended. Similarly, the IT manager should be instructed to withdraw without delay access permission to the College's computer systems.
- The investigatory officers 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 misappropriate the College's assets. any relevant laws, regulations, or other documents referenced in the policy]

Establishing and securing evidence

- The College will follow established disciplinary procedures against any member of staff who has committed fraud. The College will normally pursue the prosecution of any such individual.
- Those investigating the incident will:
 - maintain familiarity with the College's disciplinary procedures and ensure that evidence requirements will be met during any fraud investigation

- obtain approval from college management 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

Notification to DfE

- The circumstances in which the College must inform DfE about actual or suspected frauds are detailed in the Post 16 Audit Code of Practice
- The College is required to report all material fraud or irregularity to DfE where one or more of the following apply:
 - The sums involved are or are potentially in excess of £10,000
 - 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. In such cases the College may seek advice or clarification from DfE.
- 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 Committee will also be informed of the report.

Notification to Action Fraud

- 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 Department for Education (DfE) where applicable. Cyber incidents should be documented in accordance with the College's Cyber Incident Response Playbook.

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 should be sought in all cases.
- Where the loss is substantial, legal advice should be obtained without delay about the need to freeze an individual's assets through the courts pending conclusion of the investigation. Legal advice should also be sought about the prospects for recovering losses through the civil court, where the perpetrator refuses repayment. The College would normally expect to recover costs in addition to losses.
- The College may also liaise with its insurers if appropriate.

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.

Reporting to Corporation Board

- Any incident matching the criteria outlined in 5.2 shall be reported without delay to the Principal/Chief Executive, the Chair of Board, and the Chair of the Audit Committee.
- 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 Committee.
- On completion of the investigation the project group will submit to the Audit Committee a report containing:
 - a description of the incident, including the value of any loss, the people involved and the means of perpetrating the fraud
 - 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

Reporting lines during the investigation

- The project group shall provide a confidential report to the Chair of Board, the Chair of Audit Committee, and the Principal/Chief Executive. The scope of the report shall include:
 - circumstances surrounding the case and contributory factors
 - quantification of losses
 - progress with recovery action
 - progress with disciplinary action
 - progress with criminal action
 - estimate of resources required to conclude the investigation

Responsibility for investigation

- The Director of Finance shall normally lead all investigations
- Some investigations may require the use of specialists or technical expertise. In these circumstances the project group may approve the appointment of external specialists to lead or contribute to the special investigation.

Review of fraud response plan

- This plan will be reviewed for fitness of purpose at least annually or after each use. Future changes to this policy will be reported to the Audit Committee for approval
- This review will include an assessment of cyber fraud risks and the adequacy of technical controls in place to prevent and detect such incidents, as per DfE's 2025 guidance and NCSC best practice
- If any suspected fraud directly involves an officer referred to in this document, then the relevant reference should be replaced by their line manager.

6. Additional Guidance

Examples and Indicators of Fraud

Transactional Indicators

- Related party transactions with inadequate, inaccurate, or incomplete documentation or internal controls (such as business/research activities with friends, family members, or their companies)
- Not-for-profit entity has a for-profit counterpart with linked infrastructure (such as shared board of governors, 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 and or regulations, weak internal controls, a qualified audit opinion, inadequate management response to any of the above
- 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 and/or existence of pooled funds
- Unusual, complex, or new transactions, particularly if 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 (foundation set up to receive gifts) without adequate controls to determine if money or equipment has been spent/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 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, and/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 (such as small size, high value, high marketability, or lack of ownership identification) or easily diverted to personal use (such as cars, houses, equestrian centres, or villas)
- Accounts with large or frequent shifting of budgeted costs from one cost centre to another without adequate justification
- Payroll (including fringe benefits) system: controls inadequate to prevent an individual being paid twice, or paid for non-delivery or non-existence; or outsourced but poor oversight of starters, leavers, and payments
- Consultant agreements which are vague re: work, time period covered, rate of pay, product expected; lack of proof that product or service actually delivered
- Subcontract agreements which are vague re: work, time period covered, rate of pay, product expected, lack of proof that product or service actually delivered

- Sudden and/or rapid growth of newly contracted or existing education providers. For example: rapid and/or significant increase in learner numbers for newly contracted providers or providers with large cohorts of newly recruited learners in occupational areas where provider has minimal/no previous experience, concerns provider's infrastructure/staffing is insufficient to manage increase in learners

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.

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)

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 governors, directors, and/or their family members)
- Misuse of directors’ loan account facility, for example: deliberate miscoding of transactions in directors loan account to gain personal advantage
- 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

Dos and Don'ts

In addition to the warning signs outlined above, 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	DON'T
Make a note of your concerns	Be afraid of raising your concerns
<ul style="list-style-type: none"> Record all relevant details, such as the nature of your concern, the names of parties you believe to be involved, details of any telephone or other conversations with names dates and times and any witnesses. Notes do not need to be overly formal, but should be timed, signed, and dated. Timeliness is most important. The longer you delay writing up, the greater the chances of recollections becoming distorted, and the case being weakened. 	<ul style="list-style-type: none"> The Public Interest Disclosure Act provides protection for employees who raise reasonably held concerns through the appropriate channels – whistle blowing. You will not suffer discrimination or victimisation as a result of following these procedures and the matter will be treated sensitively and confidentially.
Retain any evidence that you may have	Convey your concerns to anyone other than authorised persons listed in the College's Fraud Response Plan
<ul style="list-style-type: none"> The quality of evidence is crucial and the more direct and tangible the evidence, the better the chances of an effective investigation. 	<ul style="list-style-type: none"> There may be a perfectly reasonable explanation for the events that give rise to your suspicion. Spreading unsubstantiated concerns may harm innocent persons.
Report your suspicions promptly	Approach the person you suspect or try to investigate the matter yourself
<ul style="list-style-type: none"> All concerns must be reported to the Director of Finance. 	<ul style="list-style-type: none"> There are special rules relating to the gathering of evidence for use in criminal cases. Any attempt to gather evidence by persons who are unfamiliar with these rules may undermine the case.

Anti- Fraud Checklist

Fraud occurs in every sector and providers need to be aware of the potential for it to occur. The ten questions below are intended to help providers review their arrangements for preventing,

detecting, and dealing with fraud should it occur. Arrangements will vary according to the size, structure, and complexity of the provider.

1. Are governors, accounting officer (if applicable), and chief financial officer (or equivalent) aware of the risk of fraud and their responsibilities about fraud?
2. Does the provider have a regularly reviewed counter fraud strategy, fraud risk assessment processes, and a fraud response plan?
3. Has the provider established systems and processes to respond quickly and effectively into allegations of suspected fraud, and responding to actual fraud when it arises?
4. Does the provider engender an anti-fraud culture throughout the organisation, for example: a clear statement of commitment to ethical behaviour; fraud champion; focus on prevention; sound financial regulations (including segregation of duties); recruitment; disciplinary procedures; screening; training and induction?
5. Is fraud risk included within the remit of the provider's audit committee?
6. Is fraud risk considered within the provider's risk management process?
7. Does the provider have regularly reviewed policies on whistleblowing, declarations of interest and receipt of gifts and hospitality?
8. Is it clear how and to whom suspicions of fraud in the organisation or subcontractors should be reported, both within the provider, and externally (e.g. Action Fraud, external auditors, regulators, DfE as necessary)?
9. Does the provider periodically evaluate the effectiveness of anti-fraud measures in reducing fraud?
10. Does the provider undertake 'lessons learned' exercises when suspected or actual fraud has taken place?