

Anti-Fraud and Corruption Policy

Mission Statement

WeST holds a deep-seated belief in education and lifelong learning. Effective collaboration, mutual support and professional challenge will underpin our quest to ensure that all the children and adults we serve are given every opportunity to fulfil their potential and succeed in life.

Person(s) responsible for updating the policy:	Finance Committee
Policy type:	Trust Wide
Approval level:	CFO/Deputy CFO
Date Approved:	29.04.2025
Review frequency:	Biannually
Date of Next Review:	April 2027

Contents:

1. Context	2
2. Scope	3
3. Policy Statement	3
4. Prevention	4
4.1. Risks	5
4.2. Procedures/Systems to deal with risks	5
4.3. Leadership	5
4.4. Developing and promoting an Anti-fraud culture	5
4.5. Prosecution of offenders	6
4.6. Employee Screening	6
4.7. The Role of Auditors	7
5. Detection and Reporting of Suspected Financial Irregularity	7
5.1. Internal Management Systems	7
5.2. Public Interest Disclosure ('Whistleblowing') Procedure	7
5.3. Potentially Suspicious Behaviour	8
6. Investigation of Suspected Irregularity	8
7. Recovery of losses	9
8. Monitoring and Review	9

1. Context

- 1.1 Westcountry Schools Trust takes fraud, theft, bribery, and corruption very seriously and there is a 'zero tolerance' culture to fraud in the Trust. The Trust has implemented this policy which, working alongside a set of financial policies, will ensure that arrangements are in place to protect public money.
- 1.2 To ensure that local practice and procedure learns from other instances of fraud and theft outside of the Trust, this policy will be reviewed on a two-year cycle. Where there are any instances of fraud/theft within the Trust, this policy will be reviewed as a priority
- 1.3 The Academies Handbook (AH) requires academy trusts to have an internal control framework which reduces the risk of fraud and theft. The following internal control framework and policies reduce the risks:
- Scheme of Delegation
 - Financial Scheme of Delegation;
 - Financial Regulations Manual;
 - Whistleblowing Policy;
 - Gifts and Hospitality Policy;
 - Conflicts of Interest and Related Party Transactions Policy;
 - Cyber Security Policy
 - HR Code of Conduct; and
 - Disciplinary Policies and Procedures.

1.4 Sections 6.9-6.15 of the AH refers to the investigation of fraud, theft and/or irregularity: 'Academy trusts must be aware of the risk of fraud, theft and/or irregularity and address it by putting in place proportionate controls. Trusts must take appropriate action where fraud, theft and/or irregularity is suspected or identified. The board of trustees must notify ESFA, as soon as possible, of any instances of fraud, theft and/or irregularity exceeding £5,000 individually, or £5,000 cumulatively in any financial year. Unusual or systematic fraud, regardless of value, must also be reported.'

1.5 The following information is required:

- full details of the event(s) with dates;
- the financial value of the loss;
- measures taken by the trust to prevent recurrence;
- whether it was referred to the police (and if not why); and
- whether insurance or the RPA have offset any loss.

1.6 ESFA may conduct or commission investigations into actual or potential fraud, theft, or irregularity in any academy trust, either because of a notification from the trust itself or from other information received. ESFA may involve other authorities, including the police.

1.7 Academy trusts must also be aware of the risks of cyber-crime, put in place proportionate controls and take appropriate action where a cyber security incident has occurred. Trusts should take appropriate action to meet DfE cyber security standards, which were developed to help them improve their resilience to cyber-attacks. The Trust's response is set out in its Cyber Security Policy which gives more details on how the Trust manages the threat of cyber-crime.

1.8 Trusts must obtain permission from ESFA to pay any cyber ransom demands. ESFA supports the National Crime Agency's recommendation not to encourage, endorse or condone the payment of ransom demands.' 

2 Scope

2.1 This policy relates to all academy schools and settings across the Trust (including the WeST Training Institute) and supersedes any local policies and procedures that have been in use prior to conversion.

3 Policy Statement

3.1 The Trust and its constituent academies have a duty to protect public assets; to ensure that management and other practices accord with the standards of probity expected of public sector bodies; and to ensure that the resources available to it are used only in furtherance of the Trust's objectives as an educational body. Fraud, corruption, or any other kind of financial misconduct or irregularity will not be tolerated.

3.2 An irregularity may be defined as any breach of the standards of financial integrity required by an academy and/or Trust, including a breach of the Financial Regulations. This includes any instance which has been made possible due to the actions or inactions of a member of staff even if there was no gain to them.

3.3 Irregularities fall broadly within the following categories, the first three of which are criminal, as well as disciplinary, offences (person' includes corporate bodies, including limited companies, local authorities, other employees, and students):

- Theft: the dishonest taking of property belonging to another with the intention of depriving that person permanently of its possession;
- Fraud: the intentional distortion of financial statements or other records by persons external or internal to an academy and/or Trust, to conceal the misappropriation of assets or otherwise. This includes the distortion of records to conceal losses caused accidentally or by a third party;
- Bribery: the receiving of an inducement for an action which is illegal, unethical or in breach of trust;
- Corruption: the offering, giving, soliciting or acceptance of an inducement or reward that may influence the actions of any person. Both parties are equally guilty of an offence; and
- Other irregularity: failure to observe an academy's and/or Trust's Financial Regulations, policies, and procedures. This includes failure to take appropriate action after becoming aware of such failure by another person.

3.4 The Trust has reviewed the list of generic indicators for potential fraud issued by the ESFA and assessed its risks against these indicators. It also reviews annually the ESFA fraud checklist and the Charity Commission for England and Wales's Internal Financial Controls Checklist (CC8) to provide assurance of the Trust's arrangements for preventing, detecting, and dealing with fraud should it occur and in the development of this policy.

3.5 The Trust's Internal Audit work programme supports where appropriate the prevention and identification of fraud including cybercrime.

3.6 The aftermath of financial misconduct is costly, time-consuming, disruptive, and unpleasant. The major thrust of the Trusts' strategy is, therefore, prevention.

4. Prevention

4.1 Risks

4.1.1 The largest irregularities in educational establishments typically have involved regular misappropriations over a period of years. The four areas most vulnerable to fraud in schools are cash handling, cheque handling, credit card handling and purchasing.

4.1.2 The misuse of information technology is also a major risk and one that is potentially growing in importance with the increasing reliance on technology in the education sector.

4.2 Procedures/Systems to deal with risks

4.2.1 Fraud can be minimised through carefully designed and consistently operated management procedures, in particular, financial policies and procedures and financial regulations. The Trust will therefore ensure that management procedures, as described below, are effective and that staff receive training in the operation of them.

4.2.2 Key themes of the Trust's management procedures are:

- Segregation of duties in use of financial systems is practiced, so, for example, no individual has undue management of payments, income, or assets;
- The Trust and its academies have clear roles and responsibilities, with set levels of authority for authorising transactions (the Financial Scheme of Delegation); and
- Systems are protected with electronic access restrictions to prevent the possible misuse of information technology including where possible multifactor authentication.

4.3 Leadership

4.3.1 Key determinants of behavioral standards in any organisation will be the standards observed by its senior members of staff, and the policies and approach to their enforcement. The Trust Board and its Committees, Executive, and senior managers should therefore ensure that their behavior is always demonstrably exemplary.

4.4 Developing and promoting an Anti-fraud culture

4.4.1 The Trust's Chief Financial Officer ('CFO') shall ensure all School Business Support Teams are provided, and are familiar, with the Trust's Financial Regulations Manual and the Financial Scheme of Delegation; and where necessary the ESFA's AH and published resources to reduce the risk of fraud or financial irregularities.

4.4.2 Staff will be asked to undertake training in both fraud and cyber-security where appropriate. The Trust will run phishing tests and support those staff who fail these tests with additional training.

4.4.3 The Trust has confirmed the routes for staff to report suspicions of fraud through the Trust's Whistleblowing Policy, It will respond quickly and effectively to fraud when it arises and will work with its Internal Audit function to advise the Trust Board and Audit and Risk Committee of the effectiveness of anti-fraud measures and on fraud risk.

4.5 Prosecution of offenders

4.5.1 The Police advise that prosecution is a particularly effective deterrent because of the risk of a custodial sentence and a criminal record. However, the threat of prosecution only deters if the threat is real. Therefore, the policy is that the academy and/or Trust reserves the right to report to the Police, irrespective of the status of the individual. Action taken will be underpinned by the Trust's Disciplinary Policy and Procedure.

4.6 Employee Screening

4.6.1 In line with the Trust's recruitment and selection policy, new members of staff are subject to a number of pre-employment checks:

- References from the previous two employers covering at least the previous three years' employment history will be taken up. References should be scrutinised, and any concerns resolved satisfactorily, before the appointment is confirmed, including for any internal candidate. They should always be requested directly from the referee and preferably from a senior person with appropriate authority, not just a colleague. The Trust does not accept open references. Where electronic references are received, they are verified to ensure they originate from a legitimate source. WeST policy requirements are that all references are followed up by telephone. References will be followed up if information is missing or insufficient and compared for consistency against information provided by the candidate. Any information about past disciplinary actions or allegations will be considered carefully when assessing the candidate's suitability for the post. seeking explanation of any anomalies or gaps in employment;
- Proof of the candidate's identity and eligibility to work in the UK;
- verification of qualifications / professional status/membership;
- On-line checks;
- Section 128 check (where applicable);
- A structured, robust interview process;
- verification of successful completion of statutory induction period (teaching posts) or probationary period (non-teaching); and
- DBS checks.

4.6.2 Recruitment processes require that if a member of staff has a close personal or familial relationship with an applicant, they declare this. It would be normal protocol for the member of staff to avoid any involvement in the recruitment and selection process.

4.7 The Role of Auditors

- 4.7.2 The Trust's Accounting Officer and CFO consult widely, seeking any necessary audit advice on improving the prevention or detection of fraud when new systems are being designed or existing systems are to be modified. Auditors will have regard to fraud preventative measures as part of their ongoing work
- 4.7.3 The external auditor's reviews of financial checks and balances and validation testing provide further deterrence. Auditors may also wish to assess systems in place to deter corruption.
- 4.7.4 Both internal and external auditors have a full right of access at all reasonable times to all academy and Trust properties, assets, documents, and financial and other records. The auditors are also entitled to seek explanations from any member of the academy and/or Trust's staff

5 Detection and Reporting of Suspected Financial Irregularity

5.1 Internal Management Systems

- 5.1.2 Efficient management systems are imperative if fraud is to be detected rapidly. The systematic review of every transaction minimises the risk of processing an irregular transaction. Detective checks and balances will be designed into all systems and applied consistently. This includes segregation of duties, reconciliation procedures, random checking of transactions, and review of management accounting information

5.2 Public Interest Disclosure ('Whistleblowing') Procedure

- 5.2.2 If an individual has reason to suspect that fraud is taking place (or has taken place), they are expected to bring it to the attention of senior management within the academy and/or Trust as described in the Trust's Whistleblowing Policy. This sets out to whom an individual should report their suspicions, and the protection offered to employees raising such a suspicion.

5.3 Potentially Suspicious Behaviour

5.3.1 Staff members who have committed serious financial irregularities may attempt to conceal this by rarely taking holidays, regularly working alone late or at weekends, being resistant to delegation or resenting questions about work. If any suspicions are raised, they should be discussed with the Accounting Officer, Headteacher/Principal or CFO. Any indication that a member of staff may be addicted to drugs, alcohol or gambling should also be discussed with the Accounting Officer, Headteacher/Principal or CFO. This is both for the welfare of the individual and to minimise the risks to the academy and/or Trust, which might include fraud. Any action should be taken with an assessment of the scale of risk in mind. Any suspicion will be investigated and dealt with in accordance with the procedure described below.

6. Investigation of Suspected Irregularity

6.1 Once an irregularity is suspected, reported, or disclosed, whether it relates to fraud, a whistleblowing disclosure, or an ethical issue, it is critical that any investigation is conducted in a professional manner; and in accordance with the Trust's Fraud Response Plan set out in Appendix 1 and with reference to the trust's disciplinary process and procedure where appropriate

6.2 Suspicions must be reported without delay (normally to include, the CFO). Actions taken may include one or more of the following:

- immediate reference to an appropriate external authority such as the Police or a professional body;
- Immediate engagement of HR advice and support where employee misconduct is alleged;
- appointment of an Investigating Officer, with the appropriate expertise and seniority. Decisions will be made on the remit of the investigation, form, and scope of the concluding report;
- appointment of technical or external specialists;
- in serious cases, suspension (with HR advice) whilst investigation is underway (This is a neutral act intended to facilitate enquires and does not imply any presumption of guilt). IT access is also likely to be immediately withdrawn; and
- investigations into other systems through which the suspect may have had opportunities to misappropriate assets.

6.3 The report of the investigation may conclude that there is no case to answer, that disciplinary procedures should be applied or that there should be further investigation.

6.4 In all but trivial cases, the Audit and Risk Committee will be advised of the investigation.

6.5 At the appropriate time, the Trust's insurers and external auditors will also be advised.

7. Recovery of losses

- 7.1 The Investigating Officer shall, where possible, quantify the amount of any loss. The CFO, in collaboration with the Accounting Officer, shall consider whether to, and how to go about, seeking repayment of losses.
- 7.2 Where the loss is substantial, legal advice will be obtained. The Trust would normally expect to recover costs in addition to losses.

8. Monitoring and Review

- 8.1 The Finance Committee has the responsibility for implementing, monitoring and reviewing this policy in conjunction with the Audit and Risk Committee. The CFO will make and report to both committees at each meeting of all issues raised and any subsequent actions taken. Any issues arising which do not fall within the remit of these two committees will be brought to the attention of the relevant committees and /or individuals.

Adoption of the Policy

This Policy has been adopted by the trustees of the Westcountry Schools Trust.

Signed

(Chair of Trust)

Date: 29.04.2025

APPENDIX 1



Fraud Response Plan

Date of Policy Approval:
Owner of Policy:
Authorised By:
Policy Review Date:

Chief Financial Officer
Finance Committee
29 April 2025

Contents:

Introduction	11
Reporting Fraud and/or Theft	11
Investigating Officer	11
Managing the investigation	12
Gathering evidence and interview procedure	12
Drawing matters to a conclusion	13

1. Introduction

1.1 This document provides direction in circumstances where the Trust finds itself having to deal with suspected cases of theft, fraud or corruption. It provides a framework of procedures to ensure evidence is gathered and collated to:

1.1.1 facilitate informed decisions and

1.1.2 ensure evidence gathered is admissible in future criminal or civil actions.

2. Reporting Fraud and/or Theft

2.1 If fraud is suspected, you should:

2.1.1 discuss matters with your line manager / Headteacher; or

2.1.2 with the School Business Accountant (SBA) / Chief Financial Officer (CFO which term shall include his/her appointed Deputy)); and

2.1.3 consider whether any actions are required to protect Trust IT systems (e.g. in the event of a cyber or spoofing incident).

2.2 If suspicions are grounded, the CFO will always be informed and take initial responsibility for the investigation. The CFO will consider the need to advise the Bank, mindful of the need for immediate action where funds have been misapplied.

2.3 The CFO will consider the need to inform the Chief Executive Officer (CEO which term shall include his/her appointed Deputy), Executive Leadership Team (ELT), auditors, police, ESFA and RPA. In all but trivial cases of fraud / theft, the Audit and Risk Committee and Board of Trustees are to be advised without delay.



2.4 The CFO will record details for review by the Audit and Risk Committee. The record will include all reported suspicions, including those dismissed as minor or otherwise not investigated. The record will contain details of actions taken and conclusions reached and will be presented to the Audit and Risk Committee for inspection as necessary (eg. following an incident being reported).

2.5 Where applicable, the CFO will initiate action to limit loss, and correct any weaknesses in controls, or supervision.

2.6 While responsibility remains with the CFO and CEO depending on the gravity of the suspicions, investigation may be delegated, e.g. to internal auditors, a manager, or an appropriate professional.

2.7 All staff have a responsibility to protect Trust assets and data as far as possible, within the bounds of their role.

3. Investigating Officer

3.1 An Investigating Officer will be appointed. The Investigating Officer will be assigned on a case-by-case basis and must be advised/supported by a designated member of the HR Team, who will ensure compliance with the trust's Disciplinary Policy and Procedure throughout.

3.2 The Investigating Officer will:

3.2.1 initiate a diary of events to record the progress of investigation.

- 3.2.2 Agree objectives, scope and timescale of the investigation and resources required at the outset.
- 3.2.3 Ensure that proper records are kept, including accurate notes of when, where and from whom evidence was obtained.

4. Managing the Investigation

- 4.1 The investigation will try to establish at an early stage whether a criminal act has taken place. This will shape the way that the investigation is handled and determine the likely outcome and course of action.
- 4.2 If a criminal act has not taken place, an internal investigation will be undertaken to determine the facts, consider action and recovery of any losses, and to identify system weaknesses. The CFO will maintain records of actions and report as necessary to the Audit and Risk Committee.
- 4.3 In each case the CFO and line manager will liaise with HR to ensure disciplinary procedures are followed. Where it is cost effective, civil action will be pursued to recover any losses through reference to legal advisers.
- 4.4 Where a criminal act has taken place, contact will be made with the police and legal advisers at once. The advice of the police will be followed in taking forward the investigation. Initial reports should be made to 'action fraud' www.actionfraud.police.uk (0300 123 2040), following up with a telephone conversation depending on the materiality of losses.
- 4.5 Where there are sufficient grounds, the Trust will, in addition to seeking recovery of losses, seek a criminal prosecution.
- 4.6 Where appropriate, the CFO will consider the possibility of recovering losses from insurers.

5. Gathering evidence and interview procedure

- 5.1 The Investigating Officer will interview witnesses and gather any advice, seeking professional advice as necessary. Where there are grounds for suspicion, the police will be involved at an early stage albeit that Trust staff may conduct investigations on their behalf, by agreement with the CFO and CEO.
- 5.2 In cases of spoofing or cyber, investigators should take immediate action to lock accounts, and be aware of the potential of inadvertently communicating with an impersonator (spoofing incidents).
- 5.3 If a witness is prepared to give a written statement, the Investigating Officer must maintain written records. Witnesses must be asked to sign the document as a true record.
- 5.4 The Investigating Officer will take control of physical evidence and maintain a record of where, and from whom it was taken. These are to be tagged with a reference number that corresponds with the written record of the investigation.
- 5.5 Before interviewing any suspect(s), the Investigating Officer will provide a verbal or written report to the CFO and/or CEO who will consult as necessary before reaching a decision on how to proceed.

5.6 If an interview is progressed, the interview will be carried out by the nominated Investigating Officer in accordance with the Disciplinary Policy and Procedure and supported by a HR representative.

6. Drawing matters to a conclusion

6.1 Once evidence is gathered, the CFO/CEO will consider whether there is a case to review events with the police as necessary.

6.2 Consideration will be given to the need for, and level of, any disciplinary action, up to and including dismissal with reference to HR advice.

6.3 Records are to be updated accordingly.

6.4 The need to report to the ESFA is to be considered, in line with the Academy Trust Handbook.