# Anti-Fraud & Corruption Policy

| | |
|---|---|
| Policy Dated: | April 2026 |
| Adopted by Audit & Risk Committee: | April 2026 |
| Date of Next Review: | November 2026 |
| Publication Scheme | Trust Website |
| Version: | 04 |
| Extol Lead: | CFO |

## 1. Purpose and Context

The Trust is committed to the highest standards of integrity, accountability and transparency in the stewardship of public funds. Fraud, corruption, theft and irregularity divert resources away from pupils, undermine educational outcomes and damage public confidence in the academy sector.

The Trust is a large, incorporated organisation managing significant public funds across multiple academies. The scale, complexity and volume of its operations increase its exposure to the risk of fraud, corruption and cyber-crime. The Trust therefore acknowledges its heightened responsibilities to maintain strong governance, robust internal controls and an effective counter-fraud culture.

This policy reflects the requirements of the Academies Trust Handbook, Department for Education (DfE) anti-fraud guidance and wider statutory obligations, including the offence of *failure to prevent fraud* introduced by the Economic Crime and Corporate Transparency Act 2023, which may apply to large organisations.

## 2. Scope

This policy applies to all Trustees, governors, employees (permanent, temporary and agency staff), volunteers, contractors, consultants and third parties working for, or on behalf of, the Trust.

## 3. Legal and Regulatory Framework

This policy operates in accordance with the following legislation and statutory guidance (as amended from time to time):

- Fraud Act 2006
- Bribery Act 2010
- Companies Act 2006
- Public Interest Disclosure Act 1998
- Charities Act 2011
- Academies Trust Handbook
- DfE Anti-Fraud and Corruption Guidance

This policy should be read in conjunction with the Trust's Whistleblowing Policy, Financial Regulations, Code of Conduct, Gifts and Hospitality Policy, Disciplinary Policy and Risk Management arrangements.

## 4. Definitions

For the purposes of this policy:

- Fraud includes false representation, failure to disclose information and abuse of position, as defined by the Fraud Act 2006.
- Corruption is the abuse of entrusted power for private benefit.
- Bribery is the offering, giving, receiving or soliciting of an inducement intended to influence improper performance.
- Theft is the dishonest appropriation of property belonging to another with the intention to permanently deprive.

Unless otherwise stated, the term "fraud" is used throughout this policy to encompass fraud, corruption, bribery, theft and financial irregularity.

## 5. Policy Statement

The Trust operates a zero-tolerance approach to fraud, corruption and financial irregularity. Any suspected or actual incidents will be addressed promptly, investigated proportionately and reported in line with statutory, regulatory and funding requirements.

The Trust is committed to:

- preventing fraud, theft and irregularity through strong governance and internal controls;
- encouraging a culture of openness and ethical behaviour;
- ensuring concerns can be raised safely and without fear of reprisal; and
- taking appropriate disciplinary, legal and recovery action where wrongdoing is identified.

## 6. Roles and Responsibilities

### Board of Trustees

- Holds overall responsibility for ensuring effective arrangements for the prevention, detection and response to fraud and corruption.
- Ensures compliance with the Academies Trust Handbook and DfE expectations, including reporting obligations.

Audit and Risk Committee

- Provides oversight of fraud risk management, internal controls and counter-fraud arrangements.
- Reviews reports of fraud, theft or irregularity and monitors the implementation of lessons learned.

Accounting Officer / Chief Executive Officer

- Is personally responsible for safeguarding public funds and ensuring the Trust uses resources with regularity, propriety and value for money.
- Ensures appropriate internal controls are in place to manage fraud and cyber-crime risk.
- Ensures that reportable matters are notified to the DfE promptly and accurately.

Chief Finance Officer

- Leads on fraud risk assessment, financial controls and financial irregularity matters.
- Supports investigations and reporting, working with the CEO as appropriate.

All employees and third parties

- Must act with honesty, integrity and probity.
- Are required to be vigilant to the risk of fraud and to report concerns immediately.

## 7. Prevention and Control

In line with its size and risk profile, the Trust will put in place proportionate controls to address the risk of fraud, theft, irregularity and cyber-crime. These include:

- a clear framework of delegated authority and segregation of duties;
- robust financial regulations and procurement procedures;
- declarations and active management of conflicts of interest;
- appropriate due diligence on suppliers, partners and contractors;
- regular review of fraud risks through the Trust's risk register and internal assurance activity; and
- proportionate and ongoing fraud awareness training.

## 8. Reporting Concerns

Any suspicion or allegation of fraud, theft, corruption or financial irregularity must be reported immediately via one of the following routes:

- the Chief Executive Officer;
- the Chief Finance Officer;
- the Chair of Trustees; or
- the Trust's Whistleblowing Policy.

Individuals must not attempt to investigate matters themselves. All concerns raised in good faith will be taken seriously and handled confidentially. Victimisation of whistleblowers will not be tolerated.

## 9. Reporting to the Department for Education

In accordance with the Academies Trust Handbook:

- The Trust must be aware of the risk of fraud, theft and irregularity and must address these risks by putting in place proportionate controls.
- The Trust must take appropriate action where fraud, theft or irregularity is suspected or identified.

The Board of Trustees must notify the DfE as soon as possible of:

- all instances of fraud, theft or irregularity exceeding £5,000 individually, or £5,000 cumulatively in any financial year; and
- unusual or systematic fraud, regardless of value.

Reports to the DfE must include:

- full details of the events, including dates;
- the financial value of the loss;
- measures taken to prevent recurrence;
- whether the matter has been referred to the police (and if not, the reasons why); and
- whether insurance or the Risk Protection Arrangement (RPA) has offset any loss.

The Trust recognises that the DfE may conduct or commission investigations into actual or potential fraud, theft or irregularity and may involve other authorities, including the police. The Trust further acknowledges that the DfE publishes reports relating to its investigations and financial management and governance reviews, and that these findings should inform the Trust's ongoing risk management approach.

## 10. Cyber-Crime and Cyber Security

The Trust recognises cyber-crime as a significant and growing fraud risk. In line with the Academies Trust Handbook, the Trust will:

- be aware of cyber-crime risks and maintain proportionate technical and organisational controls;
- take appropriate action in response to any cyber security incident;
- work towards meeting DfE cyber security standards to strengthen resilience against cyber-attacks.

The Trust must not pay cyber ransom demands. The Trust supports the National Crime Agency's recommendation not to encourage, endorse or condone the payment of ransoms, recognising that payment offers no guarantee of restoring access and increases the likelihood of repeat incidents.

## 11. Investigation, Sanctions and Recovery

All allegations of fraud or corruption will be assessed promptly and investigated proportionately. Where fraud is proven, the Trust will pursue appropriate disciplinary, contractual, civil and/or criminal action and seek to recover losses wherever possible.

## 12. Review

This policy will be reviewed at least annually by the Chief Executive Officer and Chief Finance Officer, and sooner where required by changes in legislation, DfE guidance or the Trust's risk profile.

## Appendix A – Indicators of Potential Fraud, Theft and Irregularity

This appendix provides non-exhaustive indicators that may suggest fraud, theft, corruption, financial irregularity or cyber-related fraud. The presence of one indicator does not, in itself, prove wrongdoing, but patterns or combinations of indicators should be treated as potential red flags and reported in line with this policy.

### 1. Behavioural Indicators (Individuals)

- Unexplained changes in behaviour, working patterns or lifestyle.
- Reluctance to take annual leave, share duties or allow review of work.
- Resistance to scrutiny, challenge or routine checks.
- Unusually close relationships with suppliers, contractors or other third parties.
- Failure to declare, or attempts to conceal, conflicts of interest.

### 2. Financial and Transactional Indicators

- Payments made outside normal processes or without appropriate approval.
- Duplicate, altered or sequential invoices with minimal supporting evidence.
- Unexplained variations between budget, forecast and actual expenditure.
- Round-sum payments or frequent journal adjustments without clear rationale.
- Purchase orders or contracts split to bypass approval thresholds.
- Payroll anomalies, including payments to unknown individuals or continued payments to leavers.

### 3. Procurement and Contracting Indicators

- Single-supplier arrangements without clear justification.
- Repeated contract awards to the same supplier despite poor performance.
- Suppliers created or amended urgently, particularly changes to bank details.
- Limited evidence of delivery for goods or services invoiced.
- Consultants or contractors engaged under vague scopes or deliverables.

### 4. Governance and Control Weakness Indicators

- Poor segregation of duties or excessive reliance on one individual.
- Lack of timely reconciliations or review of financial information.
- Incomplete or inconsistent record-keeping.
- Weak oversight or limited reporting to senior leaders or trustees.

### 5. Cyber and Technology-Related Indicators

- Unexpected requests to change bank details or make urgent payments.

- Emails or messages that appear unusual, pressurised or inconsistent with normal practice.
- Login activity at unusual times or from unexpected locations.
- Unauthorised system access, disabled controls or unexplained data changes.
- Incidents involving phishing, impersonation or ransomware attempts.

## 6. Organisational Risk Indicators

- Increased financial pressure or rapid organisational change.
- Expansion of operations without commensurate strengthening of controls.
- Repeated audit findings or failure to implement agreed actions.
- Any concerns arising from the indicators above must be reported promptly in accordance with Section 8 of this policy. Individuals must not investigate matters themselves.