



# Anti-Fraud Policy

## Document Control:

This document has been approved for operation within:	Apex Collaborative Trust		
Status	Statutory		
Owner	Alan O'Reilly (Chief Financial Officer)		
Date effective from	Nov 2025	Date of next review	Oct 2027
Review period	Two yearly	Version	1

Version	Changes identified

## **1 Statement of Intent**

1.1 Apex Collaborative Trust ('the trust') is committed to operating with the highest ethical standards and acting with integrity in all activities. The risks of fraud, theft, irregularity and cyber-crime are taken seriously, and proportionate controls will be implemented to mitigate the risks.

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

1.3 The trust will actively pursue all instances of fraud, corruption, or financial irregularity, acting in the best interests of our pupils, staff, and community.

## **2 Policy Framework**

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

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

2.2 This policy operates in conjunction with the following school policies:

- Whistleblowing Policy
- Financial Regulations Manual
- Gifts, and Hospitality Policy
- Staff Disciplinary Policy
- Staff Code of Conduct
- Cyber-security Policy

## **3 Key Definitions**

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

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

3.2 Other offences under the Fraud Act include the possession of, and the making or supplying of, articles for use in fraud. Articles would include lists of other people's credit card details or software used for producing blank utility bills or for generating credit card numbers.

3.3 Fraud can be committed in three ways according to the Fraud Act 2006:

- By false representation
- By failing to disclose information
- By abusing a position in which a person is expected to safeguard financial interests of another person

3.4 **Corruption** is the offering, giving, soliciting or accepting of any inducement or reward which may influence the actions taken by the body, its members or officers. This is the abuse of entrusted power or position for private gain.

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

3.6 **Bribery** is defined as the offering, promising, giving, accepting or soliciting of an advantage as an inducement for an action which is illegal, unethical or a breach of trust. Inducements can take the form of gifts, loans, fees, rewards or other advantages.

## 4 Roles and Responsibilities

4.1 The trust must take appropriate action where fraud, theft or irregularity is suspected or identified.

4.2 The **Chair of Trustees** is responsible for:

- Receiving reports of fraud that involve the Accounting Officer.
- Ensuring the Department for Education ('DfE') is notified as soon as possible in relation to instances of fraud, theft and irregularity:
  - Exceeding £5,000 individually,
  - Exceeding £5,000 cumulatively in any financial year, or
  - Unusual or systematic fraud, regardless of value, must also be reported.

4.3 The **Audit and Risk Committee** is responsible for:

- Ensuring that risks are being identified, addressed appropriately.
- Overseeing the trust risk register.
- Overseeing and approving the trust's programme of internal scrutiny.

4.4 The responsibilities of the **Accounting Officer** include:

- Overseeing the development and implementation of a system of internal controls that aim to minimise the risk of fraud.
- Ensuring that rigorous investigations of potential fraud are carried out promptly.
- Ensuring the appropriate legal and/or disciplinary action is taken where fraud is proven.
- Assuring the Board of Trustees that the trust is complying with the funding agreement and Academy Trust Handbook.

4.5 The responsibilities of the **Chief Financial Officer** include:

- Overseeing the financial transactions and the development and implementation of effective financial regulations, policies and procedures to prevent losses and misuse.
- Ensuring bank accounts, financial systems and financial records are operated by more than one person.

- Ensuring resources are being managed in an ethical, efficient and economical manner.
- Ensuring that appropriate action is taken to recover assets and minimise loss.
- Keeping full and accurate accounting records and producing the trust's annual accounts, including a statement on regularity, propriety and compliance.
- Assessing the areas of the trust that are most vulnerable to fraud, in conjunction with the Accounting Officer and the audit committee.
- Conducting an initial investigation where a report of fraud is made.
- Contacting the DfE to request prior approval for any transactions beyond the trust's delegation limits, and transactions that are novel, contentious or repercussive.
- Ensuring anti-fraud training is suitable and sufficient for staff across the trust.
- Maintaining registers of interests and gifts and hospitality.

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

4.7 The **internal scrutineer** will be responsible for carrying out reviews of the effectiveness and operation of the trust's systems and processes of internal control. The work of the internal scrutineer will be directed by the Audit and Risk Committee. The internal scrutineer will provide reports to the Audit and Risk Committee following each review and an annual summary of their work.

4.8 **All staff** have the responsibilities below:

- Demonstrating the highest standards of honesty, probity, openness and integrity in the discharge of their duties.
- Complying with the provisions outlined in this policy.
- Being vigilant to the risks and indicators of fraud.
- Promoting an ethical, anti-fraud culture.
- Reporting their concerns in relation to fraud or a breach of this policy to all of the above responsible individuals as appropriate.
- Providing information about any conflicts of interest and direct or indirect pecuniary interests to the headteacher.
- Maintaining the trust's estate in a safe working condition.

## 5 Indicators of Potential Fraud

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

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

## **6 Preventing Fraud**

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

6.2 Overarching anti-fraud awareness training will be available for all employees. Role-specific training will also be provided to employees with responsibility for the trust's internal controls or financial procedures.

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

6.4 The Chief Financial Officer will assess the areas of the trust that are most vulnerable to fraud risks on an annual basis. As part of this assessment, the fraud risk assessment (appendix one) will be updated. Fraud risks will be identified and will be assessed in terms of impact and likelihood.

6.5 Robust internal controls are in place to manage the risk of fraud. These cover areas including the following:

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

6.6 All employees must follow the Staff Code of Conduct and are required to declare any business or pecuniary interests, or other conflicts of interest. Trustees will be required to declare conflicts of interest using the trust's governance platform, GovernorHub.

6.7 Following a case of fraud, the trust's arrangements will be reviewed to ensure they consider all relevant risks and that the internal controls are effective.

6.8 The arrangements for financial record keeping are set out in detail in the Financial Regulations Manual.

6.9 The trust's Gifts and Hospitality policy sets out the arrangements in this area.

## 7 Reporting Concerns and Making Allegations

7.1 Allegations or concerns about suspected fraud must be reported as per the table below:

Allegations involving:	Report to:
Any member of staff	Chief Financial Officer
Chief Financial Officer	Chief Executive or Chair of Trustees
Chief Executive Officer	Chair of Trustees
Trustees	Chief Executive Officer

7.2 Staff should not investigate the concern themselves.

7.3 Staff can also follow the procedures outlined in the Whistleblowing Policy to report concerns.

7.4 Staff, volunteers and third parties can also report allegations or concerns about suspected fraud directly to the DfE using an online [enquiry form](#).

## 8 Investigating reports

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

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

8.3 Reports will be initially investigated by the Chief Financial Officer, who will ascertain the facts of the report, seeking HR and legal advice as necessary. The Chief Financial Officer will notify the Chair of Trustees of any serious financial irregularities at the first opportunity following the completion of an initial investigation.

8.4 The Chief Financial Officer will report the matter to the Chief Executive Officer and the Chair of Trustees to ensure they can discharge their own responsibilities to report instances of fraud.

8.5 Depending on the nature of a concern or report, an investigations will be carried out in accordance with the provisions relating to investigations in either the trust's Disciplinary and Dismissal Policy or Whistleblowing Policy.

## **9 Reporting to the DfE**

9.1 The Chair of Trustees will report any instances of fraud, theft and/or irregularity exceeding £5,000 individually, or £5,000 cumulatively in any financial year, to the DfE as soon as possible. Unusual or systematic fraud, regardless of value, will also be reported.

When making a report to the DfE, the following information will be provided:

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

## **10 Following an investigation**

10.1 Following an investigation, appropriate criminal, civil and disciplinary sanctions may be given in all cases of proven fraud and corruption. Where fraud involving an employee is proven, this constitutes gross misconduct and cases will be dealt with accordingly, in line with the Disciplinary Policy and Procedure.

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

10.3 Where appropriate, cases will be referred to the police in order for them to consider taking criminal action. Some instances of suspected fraud will be reported to the police at an early stage of the investigation rather than afterwards. This course of action may be taken where the initial investigation determines there is a strong likelihood of criminal activity involved.

10.4 Following any incident of fraud, a 'lessons learned' exercise will be conducted, which will aim to identify areas of internal controls or other procedures that should be improved to prevent further cases occurring.

## **11 Confidentiality**

11.1 Victimisation or harassment of anyone who has made a report will not be tolerated.

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

11.3 Concerns raised will be handled in accordance with the Whistleblowing Policy. Whistleblowers will be permitted to request confidentiality and must say straight away if they do not want anyone else to know it was them who raised the concern. In such cases every effort will be taken to protect the identity of the whistleblower.

11.4 Whistleblowers will be kept informed about the action being taken to deal with their concern. The level of detail provided may be limited if the confidence of other people needs to be maintained.

## **12 Annual accounts**

12.1 The Accounting Officer will submit the trust's annual accounts return to the DfE each year. These accounts will include the Accounting Officer's statement on regularity, propriety and compliance.

12.2 The Accounting Officer will include any identified cases of fraud in the statement. The annual audited accounts will be:

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

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

## **13 Money laundering**

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

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

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

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

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

13.5 Any concerns held by staff relating to money laundering must be raised with the Chief Financial Officer who will liaise with the Accounting Officer. Where the trust knows or suspects that an individual or organisation is engaged in money laundering or dealing in criminal property, the Accounting Officer will submit a suspicious activity report (SAR) to the National Crime Agency.

13.6 The individual or organisation the report concerns will not be informed of the suspicion. Careful consideration will be given to the trust's relationship with the individual or organisation once the report has been submitted.

## **14 Related Party Transactions**

14.1 The trust will obtain the DfE's prior approval, using DfE's related party online form, for contracts and other agreements for the supply of goods or services to the trust by a related party agreed on or after 1 September where a contract or other agreement exceeds £40,000 in the same financial year ending on 31 August.

14.2 This approval process will not apply when contracts or agreements for goods or services are arranged between the trust and the following establishments:

- State-funded schools and colleges, including academies (this does not apply to transactions with a subsidiary of such a related party).

14.3 For the purposes of reporting to and approval by DfE, contracts and agreements with related parties do not include salaries and other payments made by the trust to a person under a contract of employment through the trust's payroll.

## **15 Cyber-crime and cyber-security**

15.1 The trust will be vigilant to cyber-crime and clear cyber-security measures and proportionate controls will be implemented, as outlined in the Cyber-security policy.

## Appendix One: Fraud Risk Assessment

This fraud risk assessment identifies key areas of fraud risk for a multi academy trust. Each risk is scored by multiplying the likelihood (1–5) by the impact (1–5), resulting in a total risk score (1–25). The higher the score, the greater the risk and priority for mitigation.

The risk assessment is reviewed and updated annually or following any significant incidents. The trust will prioritise mitigation actions for areas with the highest total scores.

- **Likelihood:** 1 (Rare) to 5 (Almost Certain)
- **Impact:** 1 (Negligible) to 5 (Severe)
- **Total Risk Score:** Likelihood x Impact (Max 25)

Area of Risk	Description	Likelihood (1–5)	Impact (1–5)	Total Risk Score (L x I)	Comments/Mitigation
Procurement Fraud	Manipulation of tendering and collusion with suppliers.	3	5	15	Segregation of duties, regular audits, transparent procurement processes.
Payroll Fraud	Fictitious employees, unauthorised overtime, or false claims.	2	4	8	Regular payroll reviews, independent checks, whistleblowing procedures.
Expense Claims Fraud	Inflated or fictitious expense claims by staff or leadership.	3	3	9	Clear expenses policy, supporting documentation required, spot checks.
Asset Misappropriation	Theft or misuse of school property, IT equipment, or resources.	2	4	8	Asset registers, restricted access, regular inventories.
Grant Fraud	Falsified data or misuse of grant funding.	2	5	10	Grant monitoring, regular reporting to trustees, external review.

Cyber Fraud & Data Breach	Phishing, ransomware, or data theft impacting sensitive information.	4	5	20	Staff training, robust IT security, incident response plan.
Conflict of Interest	Undeclared interests influencing decisions or awarding contracts.	2	4	8	Annual declarations, board oversight, regular reviews.
Bank Mandate/Payment Fraud	Fraudsters impersonating suppliers or staff to redirect payments.	3	5	15	Verification procedures, dual authorisation, anti-fraud alerts.
Cash Handling Fraud	Misappropriation of cash from events, fundraising, or school meals.	2	3	6	Minimise cash handling, regular reconciliation, spot audits.

## **Appendix Two: Potential Indicators of Fraud**

### **Personal motives for fraud**

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

### **Organisational motives for fraud**

- Organisation closely identified with, or dominated by, one individual
- Organisational governance lacks clarity, direction or substance
- Organisation experiencing financial difficulty
- Tight or unusually tight time deadlines to achieve level of outputs
- Organisation under pressure to show results, e.g. budgetary matters or exam results
- Organisation recently suffered disappointment or consequences of bad decisions
- Organisation wants to expand its scope or obtain additional funding
- Funding award or contract for services is up for renewal or continuation
- Organisation due for a site visit by auditors, Ofsted or others
- Organisation faces pressure to use or lose funds to sustain future funding levels
- Record of previous failure(s) by one or more organisational areas, associated business or key personnel
- Sudden change in organisation practice or pattern of behaviour

### **Weakness in internal controls**

- There is a general lack of transparency about how the organisation works, and its procedures and controls
- Management demonstrates a lack of attention to ethical values – including a lack of communication regarding the importance of integrity and ethics, a lack of concern about the presence of temptations and inducements to commit fraud, a lack of concern regarding instances of fraud, and no clear fraud response plan or investigation policy
- Management fails to specify and/or require appropriate levels of qualifications, experience or competence for employees
- Lack of an appropriate organisational and governance structure with defined lines of authority and reporting responsibilities
- Organisation lacks policies and communication relating to individual accountability and best practice, e.g. related to procurement, expenses, use of alcohol and declarations of interest
- Lack of personnel policies and recruitment practices

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

#### **Transactional indicators**

- Related party transactions with inadequate, inaccurate, or incomplete documentation or internal controls, e.g. business activities with friends
- Not-for-profit entity has for-profit counterpart with linked infrastructure, e.g. shared Board of Trustees, governors or other shared functions and personnel
- Specific transactions that typically receive minimal oversight
- Previous audits with findings of questioned costs, evidence of non-compliance with applicable laws or regulations, weak internal controls, a qualified audit opinion, or an inadequate management response to any of these issues
- Transactions and/or accounts which are difficult to audit and/or subject to management judgement and estimates
- Multiple sources of funding with inadequate, incomplete or poor tracking, failure to segregate funds, or existence of pooled funds

- Unusual, complex or new transactions, particularly if they occur at year end or end of reporting period
- Travel accounts with inadequate, inaccurate or incomplete documentation or poor internal controls, variances between budgeted amounts and actual costs, claims in excess of actual expenses, reimbursement for personal expenses, claims for non-existent travel, or collecting duplicate payments
- Credit card accounts with inadequate, inaccurate or incomplete documentation or internal controls such as appropriate authorisation and review
- Assets which are of a nature easily converted to cash (e.g. small size, high value, high marketability or lack of ownership identification) or easily diverted to personal use (e.g. cars or houses)
- Payroll (including fringe benefits) system has inadequate controls to prevent an individual being paid twice or paid for non-delivery or non-existence
- Payroll (including fringe benefits) system is outsourced but there is poor oversight of starters, leavers and payments
- Consultant and subcontract agreements which are vague regarding the work, time period covered, rate of pay or product expected
- There is a lack of proof that a product or service was actually delivered by a consultant or subcontractor

#### **Methods used to commit and/or conceal fraud**

Employee indicators such as:

- Eagerness to work unusual hours
- Access to or use of computers at unusual hours
- Reluctance to take leave or seek support
- Insistence on doing their job alone
- Refusal of promotion or reluctance to change their job

Auditor or employee issues such as:

- Refusal or reluctance to provide information or hand over documents
- Unreasonable explanations
- Annoyance or aggressive responses to questions or requests, in an attempt to deter auditors
- Trying to control the audit process
- Promises of cooperation followed by subsequent excuses to limit or truncate cooperation
- Offering more information than asked
- Providing a lot of information in some areas and little to none in others
- Explaining a problem by saying “we’ve always done it that way”, “someone from the government told us to do it that way” or “Mr X told us to do it that way”
- Trying to rush the audit process

#### **Record keeping, banking and other**

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

- Deviation from standard procedures, e.g. all files but one handled in a particular way
- Excessive and/or poorly evidenced journal entries, unable to provide explanation for journal entries
- Transfer to or via any type of holding or suspension account
- Inter-fund company loans to other linked organisations
- Records maintained are inadequate, not updated or not reconciled
- Failure to disclose unusual accounting practices or transactions
- Unusual accounting practices or transactions, including:
  - Uncharacteristic willingness to settle questioned costs
  - Non-serial-numbered transactions or out-of-sequence invoices or other documents
  - Creation of fictitious accounts, transactions, employees or charges
  - Writing large cheques to cash or repeatedly to a particular individual
  - Excessive or large cash transactions
  - Payroll cheques with unusual or questionable endorsements
  - Payees have similar names or addresses
  - Non-payroll cheques written to an employee
- Defining delivery needs in ways that can only be met by one source or individual
- Continued reliance on person or entity despite poor performance
- Treating non-business and/or personal goods or services as business transactions in financial records
- Materials, goods and or services fictitiously erroneously reported as purchased, and evidence has been fabricated to support the claim. This could potentially be evidenced by:
  - Repeated purchases of the same items
  - Identical items purchased in different quantities within a short time period
  - Invoices and statements used to evidence purchase facilitating duplicate transactions or payments
  - Anomalies in the format of purchase invoices
  - Goods or equipment are not used as promised, or they do not work or exist
- Legitimate business assets put to non-business or private use