ST CLARE

Catholic Multi Academy Trust

# Anti-Fraud, Bribery and Corruption Policy

| | |
|---|---|
| Policy Name | Anti-Fraud, Bribery and Corruption |
| Status | Live |
| Policy Author | Chief Financial Officer |
| Date Adopted | June 2022 |
| Review Period | 3 years |
| Last Review Date | July 2023 |
| Next Review Date | By 31 July 2026 |
| Version | 1.02 |
| Advisory Committee | Finance and Resources Committee |
| Linked Documents and Policies | Financial Regulations<br>Financial Scheme of Delegation |

This policy shall be reviewed in accordance with the above review date or earlier should there be a legal requirement, business requirement or any collective agreement that necessitates a change.

# Contents

## Introduction

St Clare Catholic Multi Academy Trust (Trust) will conduct all of its affairs in an open, transparent and ethical manner.

The Trust has a zero-tolerance approach to fraud, bribery and corruption and is committed to acting professionally, fairly and with integrity in all its business dealings and relationships wherever it operates and implementing and enforcing effective systems to counter fraud, bribery and corruption.

The Trust expects the highest standards of propriety and accountability of its Members, Trustees, staff, volunteers and other relevant stakeholders.

## Policy Statement

The purpose of this policy is to:

- set out our responsibilities, and of those working for the Trust, in observing and upholding its position on fraud, bribery and corruption; and
- provide information and guidance to those working for the Trust on how to recognise and deal with fraud, bribery and corruption issues.

This policy will describe the Trust's approach to minimising the risk of fraud, bribery and corruption and identify the importance of embedding a culture of zero tolerance.

In this policy, third party means any individual or organisation you come into contact with during the course of your work for the Trust, and includes actual and potential students, parents, caregivers, customers, suppliers, distributors, business contacts, agents, advisers, and government and public bodies, including their advisors, representatives and officials, politicians and political parties.

This policy does not form part of any employee's contract of employment and may be amended at any time to reflect changes in legislation, best practice and/or the needs of the Trust.

## Roles and Responsibilities

The prevention, detection and reporting of fraud, bribery and corruption is an inherent responsibility of all individuals and legal entities working for the Trust or on its behalf, irrespective of their capacity; including but not limited to those listed below:

- members,
- trustees,
- directors and executive officers,
- employees
- agency workers,
- external consultants,
- third-party representatives,
- partner organisations; and
- volunteers.

All individuals and legal entities are required to avoid any activity that might lead to, or suggest, a breach of this policy.

## Trustees Responsibilities

Trustees have overall responsibility for the maintenance and operation of this policy and must ensure compliance with all legal and regulatory obligations. As a minimum Trustees will ensure the following:

- ensure there are appropriate internal and financial controls in place to make sure all funds are accounted for and spent in line with the charity's aims,
- keep proper and adequate financial records for both the receipt and use of all funds together with audit trails of decisions made,
- take any actions necessary to protect charity funds,
- act responsibly and within the interests of the Trust if fraud occurs. This includes reporting incidents of fraud, bribery and corruption to the relevant authorities where appropriate, and ensuring the Trust's financial resources and assets are secure.

## Management Responsibilities

Management at all levels are responsible for the communication and implementation of this policy in their work area. Management is also responsible for ensuring that their staff are aware, understand and comply with this and all related policies and procedures and that adequate and regular training is provided.

Management is expected to create an environment where staff are able to approach them with any concerns they may have about suspected fraud, bribery and corruption. However, should a member of staff prefer; because their immediate manager is unavailable or indeed may be the cause for concern; then the Chief Financial Officer (CFO) may be approached.

All allegations of suspected fraud, bribery, corruption and/or theft brought to the attention of management should and will be:

- dealt with promptly,
- reported to the CFO,
- record all evidence received,
- ensure all immediately available evidence is sound and adequately supported,
- implement the whistleblowing and/or disciplinary policy and procedures, where appropriate.

## Staff Responsibilities

All categories of staff and/or volunteers are governed in their work by the Trust's policies and procedures including the code of conduct. Staff and/or volunteers are responsible for ensuring that they follow all instructions given to them by management, particularly in regard to the safeguarding of public funds and the resources and assets of the Trust.

Staff and/or volunteers are expected to always be aware of the possibility that fraud, bribery, corruption and/or theft may exist in the workplace therefore, all employees/volunteers should avoid the following:

- acting in any way that might cause others to allege or suspect them of dishonesty,

- behaving in a way that would not give cause for others to doubt that Trust's employees/volunteers deal fairly and impartially with official matters,
- give, promise to give, or offer, a payment, gift or hospitality with the expectation or hope that a business advantage will be received, or to reward a business advantage already given,
- give or accept a gift or hospitality during any commercial negotiations or tender process, if this could be perceived as intended or likely to influence the outcome,
- accept a payment, gift or hospitality from a third party that you know or suspect is offered with the expectation that it will provide a business advantage for them or anyone else in return,
- accept hospitality from a third party that is unduly lavish or extravagant under the circumstances,
- threaten or retaliate against another individual who has refused to commit a bribery offence or who has raised concerns under this policy; and/or
- engage in any other activity that might lead to a breach of this policy.

## Culture

The importance of a positive culture towards anti-fraud, bribery and corruption cannot be overstated.

The effectiveness of the Trust's arrangements can be undermined by a culture that does not apply recognised public standards (Appendix 1) and supporting policies and procedures routinely on a day-to-day basis.

Maintaining appropriate arrangements, continually advocating their use and taking robust action all help underpin the development of a strong culture of zero tolerance towards fraud, bribery and corruption.

The Trust will continue to assess the organisational culture and ensure it promotes the highest standards of oversight, governance and best practice.

## Facilitation Payments and Kickbacks

The Trust does not make, and will not accept, facilitation payments or "kickbacks" of any kind.

All employees/volunteers must avoid any activity that might lead to a facilitation payment or kickback being made or accepted by the Trust or on its behalf, or that might suggest that such a payment will be made or accepted.

If you are asked to make or authorise a payment on behalf of the Trust, you should always be mindful of what the payment is for and whether the amount requested is proportionate to the goods or services provided. In all instances authorised formal documentation (physical or digital) must accompany a payment request. If you have any suspicions, concerns or queries regarding a payment, you should refer these to your immediate manager or alternatively you may prefer; because your immediate manager is unavailable or indeed may be the cause for concern; to approach the CFO.

## Gifts, Hospitality and Expenses

This policy allows reasonable and appropriate hospitality or entertainment given to or received from third parties, for the purposes of:

- establishing or maintaining good business relationships,
- improving or maintaining our image or reputation, or
- marketing or presenting our products and/or services effectively.

The giving and accepting of gifts is allowed if the following requirements are met:

- it is not made with the intention of influencing a third party to obtain or retain business or a business advantage, or to reward the provision or retention of business or a business advantage, or in explicit or implicit exchange for favours or benefits,
- it is given in the name of the Trust,
- it does not include cash or a cash equivalent (such as gift certificates or vouchers),
- it is appropriate in the circumstances, taking account of the reason for the gift, its timing and value; and
- it is given openly, not secretly.

Promotional gifts of low value such as branded stationery to or from existing customers, suppliers and business partners will usually be acceptable.

Reimbursing a third party's expenses or accepting an offer to reimburse our expenses (for example, the costs of attending a meeting/conference) would not usually amount to bribery. However, a payment in excess of genuine and reasonable business expenses (such as the cost of an extended hotel stay) is not acceptable.

In determining the appropriateness of any gift and/or hospitality it is important to consider whether in all the circumstances the gift, hospitality or payment is reasonable and justifiable. The intention behind it should always be considered.

## Internal Controls and Risk Management

The Trust has a wide range of policies and procedures in place to minimise the risk of fraud, bribery, corruption and/or theft. These controls constitute a major part of the Trust's system of internal control. The system is designed to ensure all transactions are conduct in an effective and efficient manner and as far as possible prevent potential fraudsters from exploiting weaknesses.

## Key Procedures and Controls

The following key controls and procedures operate across the Trust:

- a comprehensive suite of policies and guidance regarding fraud prevention, bribery and corruption and/or theft,
- ongoing and developing programme of staff training and development,
- maintaining a culture of vigilance and a zero tolerance towards fraud, bribery or corruption,
- a register of business and pecuniary interests is maintained to identify any financial or non-financial interests that may bring about conflict with the Trust's activities and/or interests,
- a register of gifts and hospitality is maintained to record gifts and hospitality either received, or offered and declined, from any third party,
- whistleblowing procedures are in place and easily accessible to all stakeholder,
- appropriate scheme of delegated authority and financial regulations,
- robust recruitment and selection procedures,
- clear and active disciplinary arrangement; and

- recovery of losses through the civil and criminal courts or deducting losses from any salary payments.

## Deterring Fraud, Bribery and Corruption

The Trust operates a number of processes to deter potential fraudsters from committing or attempting fraudulent or corrupt acts, including bribery, whether they are inside and/or outside of the Trust:

- promoting the Trust's determination to prevent and detect fraud, bribery and corruption through centrally co-ordinated procurement pathways,
- acting robustly and decisively when fraud, bribery and corruption is suspected and proven through termination of contracts and dismissal,
- taking action to recover any losses through fraud and/or theft such as civil proceedings; and
- having sound internal control systems, which allow for innovation while limiting opportunities for fraud, bribery, corruption and theft.

The Trust has implemented a framework which identifies potential areas where fraud can occur, appendix 2.

## Independent Review

## Internal Audit

Internal auditors are appointed by the Trustees in order to secure an independent oversight of the Trust's and individual academies' financial and operational affairs. The primary function of the internal auditors is to provide the Trust with independent assurance that:

- the financial responsibilities of the Trust are being properly discharged,
- resources are being managed in an efficient, economical and effective manner,
- sound systems of internal control are being maintained; and
- financial considerations are fully taken into account in reaching decisions.

The completion of internal scrutiny reviews will ensure that standard operating controls and processes are fully implemented and are adequate to reduce the risk of fraud, corruption and/or theft.

Where fraud or corruption has occurred due to a breakdown in Trust systems and procedures, or the internal audit identifies a potential weakness in controls, the Trust will ensure that appropriate improvements in systems of control are implemented to reduce the risk of a reoccurrence.

## External Audit

The Trust's annual report and financial statements include an Independent Auditors' Report. This report includes a view as to whether the financial statements give a true and fair view and whether proper accounting records have been kept by the Trust throughout the financial year.

In addition, the external audit also provides a limited assurance report on the regularity of the Trust financial affairs, confirming resources have been applied to the purposes identified by Parliament and the financial transactions conform to the authorities which govern them.

## Reporting Allegations of Fraud, Bribery and Corruption

An allegation of fraud, bribery, corruption and/or theft may be reported if there is a reasonable belief that one or more of the following has occurred, in the process of occurring or is likely to occur:

- a criminal offence,
- a failure to comply with a statutory or legal obligation,
- improper unauthorised use of funds,
- false representation,
- failure to disclose information,
- abuse of position; and/or
- deliberate concealment or complicity in any of the above.

The Trust will ensure that any allegations received in any way, including by anonymous letter or phone call, will be taken seriously and investigated in line with the Trust's Whistleblowing Policy.

The Trust will deal firmly with individuals who engage in fraudulent activity, or who are corrupt, or where there has been financial malpractice. There is, of course, a need to ensure that any investigation process is not misused, and, therefore any abuse (such as staff raising malicious allegations) may be dealt with as a disciplinary matter.

### Response to Allegations

The Trust will seek to address any allegation of fraud, bribery, corruption and/or theft as per its Fraud Response Plan, appendix 3, which provides a framework and guide to ensure all allegations are treated in a fair and equitable manner. The framework seeks to address the following areas:

- notifying suspected fraud,
- investigation process,
- liaison with police and external audit,
- initiation of recovery action; and
- reporting process.

### Confidentiality and Safeguards

Individuals who refuse to accept or offer a bribe, or who raise concerns or report another's wrongdoing, are sometimes worried about possible repercussions. The Trust encourages openness and will support anyone who raises genuine concerns in good faith under this policy, even if they turn out to be mistaken.

The Trust is committed to ensuring no one suffers any detrimental treatment as a result of refusing to take part in bribery or corruption, or because of reporting in good faith their suspicion that an actual or potential fraud or other offence has taken place, or may take place in the future. Detrimental treatment includes dismissal, disciplinary action, threats or other unfavourable treatment connected with raising a concern. If you believe that you have suffered any such treatment, you should inform the CFO immediately. If the matter is not remedied, and you are an employee, you should raise it formally using the Trust's grievance procedure.

## Definitions

| | |
|---|---|
| Fraud | The intentional distortion of financial statements or other records by persons internal or external to the organisation which is carried out to conceal the misappropriation of assets or otherwise for gain. |
| Bribery | A financial or other advantage that is offered or requested with the intention of inducing or rewarding the improper performance of a relevant function or activity, or with the knowledge or belief that the acceptance of such an advantage would constitute the improper performance of such a function or activity. |
| Corruption | The offering, giving, soliciting or accepting of any inducement or reward which would influence the actions taken by an organisation, its members or officers. |
| Advantage | An advantage includes money, gifts, loans, fees, hospitality, services, discounts, and the award of a contract or anything else of value. |
| Improper | A person acts improperly where they act illegally, unethically, or contrary to an expectation of good faith or impartiality, or where they abuse a position of trust. The improper acts may be in relation to any business or professional activities, public functions, acts in the course of employment, or other activities by or on behalf of any organisation of any kind. |
| Facilitation Payment | Also known as "back-handers" or "grease payments" are typically small, unofficial payments made to secure or expedite a routine or necessary action. |
| Kickbacks | Typically, payments made in return for a business favour or advantage |

## Related policies, procedure and information sources

- Whistleblowing Policy
- Disciplinary Policy
- Procurement Policy
- Expenses (Staff and Trustees) Policy

## Data protection, equality and diversity

A data protection impact assessment (DPIA) and equality impact assessment (EIA) have been completed for this policy.

## Appendix 1 – Nolan Principles

### What are the seven Nolan principles?

In 1995 the Committee on Standards in Public Life, chaired by Lord Nolan, received its first report establishing the Seven Principles of Public Life. Now referred to as the 'Nolan principles', the recommendations aimed at improving standards of behaviour in public life. There are seven basic principles.

#### Selflessness

Holders of public office should act solely in terms of the public interest.

#### Integrity

Holders of public office must avoid placing themselves under any obligation to people or organisations that might try inappropriately to influence them in their work. They should not act or take decisions in order to gain financial or other material benefits for themselves, their family, or their friends. They must declare and resolve any interests and relationships.

#### Objectivity

Holders of public office must act and take decisions impartially, fairly and on merit, using the best evidence and without discrimination or bias.

#### Accountability

Holders of public office are accountable to the public for their decisions and actions and must submit themselves to the scrutiny necessary to ensure this.

#### Openness

Holders of public office should act and take decisions in an open and transparent manner. Information should not be withheld from the public unless there are clear and lawful reasons for so doing.

#### Honesty

Holders of public office should be truthful.

#### Leadership

Holders of public office should exhibit these principles in their own behaviour. They should actively promote and robustly support the principles and be willing to challenge poor behaviour wherever it occurs

## Appendix 2 – Fraud Indicators

This framework document provides a list of generic indicators of potential fraud. These include personal and organisational motives for fraud, possible weakness of governance or internal controls, transactional indicators and possible methods of concealing fraud.

### Potential Personal Motives

#### Financial motives

- personnel believe they receive inadequate pay and/or rewards,
- individuals' expensive lifestyle,
- personal problems.

#### Personal motives

- disgruntled employee (recently demoted, reprimanded etc.),
- recent failure associated with specific individual,
- personal animosity or professional jealousy,
- unusually high degree of competition/peer pressure,
- undeclared conflicts of interest or related party transactions (business activities with personal friends, relatives or their companies).

### Possible Organisational Motives

#### Financial issues

- organisation experiencing financial difficulty,
- commercial arm experiencing financial difficulty,
- organisation has for-profit component,
- not-for-profit entity has a for-profit counterpart with linked infrastructure (shared board of governors or other shared functions and personnel),
- organisation under pressure to show results (budgetary, exam results etc.),
- organisation recently suffered disappointment/reverses/consequences of bad decisions,
- organisation recently affected by new/changing operating environment,
- organisation faces pressure to use or lose funds to sustain future funding levels.

#### General

- tight or unusually tight time deadlines to achieve level of outputs,
- organisation wants to expand its scope, obtain additional funding,
- funding award up for continuation,
- organisation due for a site visit by auditors, Ofsted or others,
- record of previous failure(s) by one or more organisational areas.

### Potential Weaknesses in Management & Governance

- organisation governance lacks clarity and direction,
- organisation closely identified with/dominated by one individual,
- management demonstrates lack of attention to ethical values (e.g. Nolan principles, integrity and ethics).

### Risk management

- management fails to recognise required levels of competence in high-risk areas,
- management displays lack of commitment towards the identification and management of risks relevant to the preparation of financial statements (does not consider significance of risks, likelihood of occurrence or how they should be managed),
- management take unnecessary risks.

### Financial management

Institution lacks policies and communication relating to financial management, individual accountability, and best practices e.g.

- procurement,
- travel and subsistence,
- use of alcohol,
- declarations of interest.

### Personnel policies

- lack of personnel policies and recruitment practices,
- Institution lacks personnel performance appraisal measures or practices.

### General

- management is unaware of or displays lack of concern regarding applicable laws and regulations e.g. Companies Acts, Funding Agreement, Child Protection,
- sudden change in organisation practice or pattern of behaviour,
- lack of staff training or fraud awareness.

## Potential Internal Control Issues

### Internal Control

- lack of an appropriate organisational and governance structure with defined lines of authority and reporting responsibilities,
- lack of oversight of budget management, including comparison of budgets with actual performance and costs, forecasts and prior performance; no regular reconciliation of control records and lack of proper reporting to FARC and LAC,
- general lack of management oversight or appropriate level of challenge,
- there is inadequate or inappropriate segregation of duties regarding initiation, authorisation and recording of transactions, maintaining custody of assets,
- there is a lack of internal, independent monitoring of controls in place; failure to take any corrective actions, if needed,
- no mechanism exists to inform management and governors of possible fraud,
- management of information systems is inadequate (no policy on information technology security, computer use and access, verification of data accuracy completeness or authorisation of transactions),
- accounting systems are inadequate (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 prevent missing payment dates, etc.),

- purchasing systems/procedures inadequate (poor or incomplete documentation of purchase, payment, receipt; poor internal controls as to authorisation and segregation of duties),
- previous audits with findings of
    - questioned costs
    - evidence of non-compliance with applicable laws or regulations
    - weak internal controls
    - inadequate management response to any of above
    - a qualified opinion
- History of problems
    - Slow response to past findings or problems
    - Unresolved findings
- there is insufficient physical security over facilities, assets, records, computers, data files, cash; failure to compare existing assets with related records at reasonable intervals.

### Transactional Indicators

- related party transactions with inadequate, inaccurate or incomplete documentation or internal controls (business/research activities with friends, family members or their companies),
- specific transactions that typically receive minimal oversight,
- transactions and/or accounts which are difficult to audit or subject to management judgment and estimates,
- 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,
- Travel and subsistence accounts with:
    - inadequate, inaccurate or incomplete documentation
    - receipts not provided
    - variances between budgeted amounts and actual costs
    - claims in excess of actual expenses
    - reimbursement for personal expenses
    - claims for non-existent travel
    - collecting duplicate payments
- credit card accounts with inadequate, inaccurate or incomplete documentation or internal controls such as appropriate authorisation and review,
- consultant/ subcontract agreements which are vague as to
    - schedule of work
    - time period covered
    - rate of pay
    - product expected
- lack of proof that product or service actually delivered,
- accounts in which activities, transactions or events involve handling of cash or wire transfers; presence of high cash deposits maintained with banks,
- writing large cheques to cash or repeatedly to a particular individual, or excessive or large cash transactions,
- 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,

- accounts with large or frequent shifting of budgeted costs from one line item to another without adequate justification,
- 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 (as in a 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 such as foundation provided limited access to documentation,
- assets and inventory are of a nature to be easily converted to cash (small size, high marketability, lack of ownership identification, etc.) or easily converted to personal use (cars, houses, equestrian centres, villas etc.)

## Record Keeping/Banking

Records maintained are inadequate, not updated or reconciled. Examples:

- missing documents,
- documents are copies, not originals,
- documents in pencil,
- altered documents,
- false signatures/incorrect person signing.
- Process issues:
    - non-serial-numbered transactions or out-of-sequence invoices or other documents
    - duplicate invoices
    - creation of fictitious accounts, transactions, employees, charges
    - payroll checks with unusual/questionable endorsements
    - payees have similar names/addresses
    - non-payroll cheques written to an employee
    - excessive journal entries
    - use of several different banks, or frequent bank changes; use of several different bank accounts
    - transfers to or via any type of holding or suspension account
    - deviation from standard procedures (all files but one handled a particular way; all documents but one included in file, etc.)
- fund loans to other linked organisations,
- failure to disclose unusual accounting practices or transactions,
- defining delivery needs in ways that can only be met by one source,
- continued reliance on person/entity despite poor performance,
- materials erroneously reported as purchased; repeated purchases of same items; identical items purchased in different quantities within a short time period; equipment not used as promised, doesn't work, doesn't exist,
- charging items to project account for personal purposes (books and supplies bought for family members, home gym equipment charged to project account etc.)

## Other

### Personal behaviours:

- uncharacteristic willingness to settle questioned costs,
- eagerness to work unusual hours,

- access to/use of computers at unusual hours,
- reluctance to take leave,
- insistence on doing job alone,
- refusal of promotion or reluctance to change job.

## Potential Methods for Concealing Fraud

During an audit or when verifying transactions for approval the auditee may demonstrate some of the following behaviours:

- refusal or reluctance to turn over documents,
- unreasonable explanations,
- annoyance at questions,
- trying to control the audit process (timetables, access, scope),
- auditee 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 ESFA/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.

## Appendix 3 – Cyber Crime and Cyber Security Framework

### Home and mobile working:

- is there a clear policy on mobile working, with all associated training?
- is a secure baseline build applied to all devices?
- is data protected outside formal work environments, including in transit?

### User education and awareness:

- are there security policies in place covering acceptable and secure use of systems?
- is there a staff training programme covering secure use of systems and awareness of cyber risks – for example strengthening passwords, risk from public Wi-Fi hotspots, risks from use of removable media such as USB sticks, avoiding use of personal accounts for business purposes and maintaining backups?
- do staff know how to report issues and incidents?

### Incident management:

- does the organisation have an incident management/response plan and are these tested?
- are criminal incidents reported to law enforcement bodies?

### Information risk management regime:

- is there a governance structure for managing information risk?
- do information professionals liaise with central government, stakeholders and suppliers to understand the threat?
- does senior management understand and engage with risk mitigation processes?

### Managing user data access rights / privileges:

- are there effective account management processes, with limits on privileged accounts?
- are use privileges controlled and monitored?
- is access to activity and audit logs controlled?
- are these logs reviewed for unusual behaviour?

### Removable media controls:

- is there a policy on the use of removable media (for example, CDs, flash/pen drives, mobile phones, wireless printers) and is this implemented?
- are media scanned for malicious software (malware) before being linked to the system?

### Monitoring:

- is there a monitoring strategy in place for all information communications technology (ICT) systems and networks?
- are logs and other monitoring activities able to identify unusual activity that could indicate an attack?

### Secure configuration:

- does a system inventory exist?
- is unnecessary functionality removed or disabled from systems?
- are security patches applied regularly?

- is there a minimum defined baseline for all devices?

Malware protection:

- are there effective anti-malware defences in place across all business areas?
- is there regular scanning for malware?

Network security:

- is the network perimeter managed?
- do information professionals understand where the highest risk information assets are, and how they are protected?
- are security controls monitored, tested and where appropriate updated?

## Appendix 4 – Allegation (Fraud, Bribery & Corruption) Response Plan

### Reporting

In the first instance, any suspicion of fraud, bribery, corruption or other irregularity should be reported, as a matter of urgency, to the Chief Financial Officer (CFO). However, the issue may initially be reported upwards to the Chief Executive Officer (CEO) or Chair of ARAC, if the cause of concerns is the CFO.

Every effort will be made to protect an informant's anonymity if requested. However, the Trust will always encourage individuals to be identified to add more validity to the accusations and allow further investigations to be more effective. In certain circumstances, anonymity cannot be maintained. This will be advised to the informant prior to release of information.

### Investigation Process

All suspected incidents of fraud, bribery and corruption will be investigated in an independent, open-minded and professional manner with the aim of protecting the interests of both the Trust and the suspected individual(s).

Suspicion must not be seen as guilt to be proven.

The investigation process will vary according to the circumstances and will be determined by the CEO in consultation with the CFO and Chair of Audit Committee. An "Investigating Officer (IO)" will be appointed to take charge of the investigation on a day-to-day basis. This will normally be the CFO or, in exceptionally circumstances, another independent member of the Trust may be appointed.

The IO will appoint an investigating team. This will normally comprise staff from within the finance and human resources departments but may be supplemented with other resources within the Trust or externally.

Where initial investigations reveal that there are reasonable grounds for suspicion, and to facilitate the ongoing investigation, it may be appropriate to suspend the suspected individual(s). This decision will be taken by the CEO, CFO and the Chair of ARAC.

Suspension should not be regarded as disciplinary action nor should it imply guilt.

It is important, from the outset, to ensure that evidence is not contaminated, lost or destroyed. The investigating team will therefore take immediate steps to secure physical assets, including computers and any records thereon, and all other potentially evidential documents. They will also ensure, in consultation with management, that appropriate controls are introduced to prevent further loss.

The IO will ensure that a detailed record of the investigation is maintained which should include:

- a chronological file recording details of all telephone conversations, discussions, meetings and interviews,
- details of documents reviewed, tests and analyses undertaken, the results and their significance.

Everything should be recorded, irrespective of the apparent significance at the time.

The findings of the investigation will be reported to the CEO, CFO and the Chair of ARAC who in consultation with the Chair of Trustees, will determine what further action (if any) should be taken.

## Liaison with Police & External Audit

The police generally welcome early notification of suspected fraud, particularly that of a serious or complex nature. The Chair of Trustees, following consultation with the CEO, CFO and the Chair of ARAC will decide if and when to contact the police. The Chair of ARAC and the CFO will report suspected incidents of fraud, bribery and corruption to the external auditors at an appropriate time.

All staff will be expected to co-operate fully with any police or external audit enquiries, which may have to take precedence over any internal investigation or disciplinary process.

## Recovery Action

The Academy will take appropriate steps, including legal action, if necessary, to recover any losses arising from fraud, theft or misconduct. This may include action against third parties involved in the fraud or whose negligent actions contributed to the fraud.

## Reporting process

Throughout any investigation, the IO will keep the CEO and Chair of Audit Committee informed of progress. If the investigation is long or complex, interim reports to the Chair and Board of Trustees will be made.

Upon completion of the investigation, the IO will prepare a full written report for the Trustees setting out:

- background as to how the investigation arose,
- what action was taken in response to the allegations,
- conduct of the investigation,
- facts that came to light and the evidence in support,
- action taken against any party where the allegations were proved,
- action taken to recover any losses; and
- recommendations and/or action taken by management to reduce further exposure and to minimise any recurrence.

## Communication with the Secretary of State (ESFA)

The Trust will notify the Education Skills Funding Agency (ESFA), as soon as is operationally practical, of any instances of fraud, bribery, corruption and/or irregularity exceeding £5,000 individually, or £5,000 cumulatively in any academy financial year. Any unusual or systematic fraud, regardless of value, will also be reported.

The ESFA reserves the right to conduct or commission its own investigation into actual or potential fraud, bribery, corruption, theft or irregularity, either as the result of a formal notification from the Trust itself or as the result of other information received.