Tithe Academy

Fraud Avoidance Policy

Introduction

This policy has been formulated to comply with the Trust's Articles of Association and the Academies Financial Handbook.

In line with the Trust's Equal Opportunities and Special Educational Needs policies, we aim to give all students equal opportunities to take part in all aspects of school / college life, as far as is appropriate, practicable and compatible with giving regard to health and safety and the efficient education of other students.

This policy takes account of the Government's aim for children to have the support they need under Every Child Matters:

- to be healthy
- to stay safe
- to enjoy and achieve
- to make a positive contribution
- to achieve economic well-being

The policy will follow the five principles of the Children's Plan:

- to support parents and families
- to allow children to reach their full potential
- to enable children to enjoy their childhood whilst preparing for adult life
- to provide services in response to children and family needs
- to use preventative measures to help students avoid the possibility of failure

Recommended by the Audit & Risk Committee / Local Governing Body: 29.11.17 / 22.1.18

Approved by Board of Trustees: 5th February 2018

Revised edition: LGB 7.5.19

Foreword

Tithe Academy is comprised of Earlsmead Primary School, a mixed 4 to 11 year old primary school with specialist SEN unit, and Rooks Heath College which is a mixed 11 to 18 multicultural comprehensive in the London Borough of Harrow. It is the personal responsibility of the CEO, as Accounting Officer, to prevent loss through fraud and irregularity. The CEO has delegated responsibility for formulation of this policy to the CFO in consultation with the Trust's Finance Manager and appropriate staff. The policy is monitored by the Audit and Risk Committee. The policy is subject to annual review by the Audit and Risk Committee and is subject to approval by the Trustees.

Scope

This policy sets out the requirements for all staff (including agency staff, contractors and peripatetic teachers) in relation to the prevention and detection of fraud.

The aims of this policy

The Trust has a 'zero tolerance' to fraud and requires all staff at all times to act with probity and integrity to safeguard the public resources for which the Trust is responsible. Fraud is an ever - present threat to resources. All Trust staff must therefore remain alert to the risk that fraud or other irregularity could occur in their area of responsibility.

The purpose of this policy is to set out:

- staff responsibilities regarding the prevention of fraud and irregularity
- the procedure to be followed where a fraud or irregularity is detected or suspected.

All actions taken by Trust staff shall be in accordance with the law and relevant Trust policies and procedures.

Other documents within the Trust which help define the ethical framework within which staff are required to operate include the staff disciplinary policy, Whistle Blowing policy, Financial Procedures and staff code of conduct.

Definitions and Terminology

For clarity and transparency the following Acts and definitions are used:

Fraud

The Fraud Act 2006 came into force on 15th January 2007. The Act created a single offence of fraud and defined this in three classes:

- False representation;
- Failure to disclose information where there is a legal duty to do so;
- Abuse of position.

The Act also created four new offences of:

- Possession of articles for use in fraud;
- Making or supplying articles for use in fraud;
- Obtaining services dishonestly;
- Participating in fraudulent business.

The Chartered Institute of Public Finance and Accountancy (CIPFA)*1 defines fraud as:

"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 bribe is:

"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" [CIPFA].

There are various Bribery offences, including offering or accepting a bribe (Sections 1 and 2 of the Bribery Act 2010), bribing or attempting to bribe a foreign official (Section 6) and being a commercial organisation failing to prevent bribery (Section 7). While the Council is not a 'commercial organisation' for its normal activities, it is still considered appropriate for it to have regard to Guidance relating to the Bribery Act.

Corruption

Corruption is:

"*The offering, giving, soliciting or accepting of any inducement or reward which would influence the actions taken by the body, its members or officers."*

Theft

The 1968 Theft Act states that:

"A person shall be guilty of theft if s/he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it".

The term is usually employed to describe acts such as:

- bribery
- corruption
- forgery
- extortion
- conspiracy
- theft
- embezzlement
- misappropriation
- false representation
- concealment of material facts

For all practical purposes fraud may be defined as "The use of deception and the intention of obtaining an advantage, avoiding a loss, or causing loss to another party."

Fraud can be committed by persons outside as well as inside the Trust.

Fraud could include major systematic cases such as collusion by senior and other staff within the Trust to over claim funding from the DfE or other funding agency or organisation.

Other examples of fraud or irregularity relevant to the Trust context could include:-

- pilfering of stock
- improper use of telephone/fax facilities
- unauthorised use of Trust equipment (including computers)
- theft of cash or equipment
- improper manipulation of computer programs or data collusion with others for illicit gain
- falsification of claims for travel and subsistence or other allowances
- improper/inaccurate claims for overtime or time off in lieu
- any other impropriety.

External attempts at fraud or irregularity could include:

- offers of bribes/inducements
- submission of false invoices
- demands for payment for unsolicited goods
- contractor frauds involving overcharging, sub-standard work, bid rigging and/or collusion in competition to services
- fraudulent claims for Trust funds
- Cyber fraud including scams, phishing, vishing, malvertising, social engineering

Cyber Crime and Cyber Security

Cyber crime is described as a crime where the computer is the object of the crime or used as a tool to committing an offence. A cybercriminal may use a device to access a user's personal information, confidential business information or to disable a device. It is also a cybercrime to sell or elicit the above information online.

Cyber crime may involve malicious attacks on computer software, including:

- email hacking, which is unauthorised access to an email account by tricking people to open or respond to spam emails or to open emails with a virus;
- phishing, which involves hackers sending malicious email attachments or URLs to users to gain access to their accounts or computers. Users are tricked into emails claiming they need to change their passwords or updating their payment details, giving criminals access;
- Malvertising, which is online advertising, which looks harmless, but may lead to harmful content or may directly infect the victim's computer with malicious software

that can damage data or steal personal information or even bring the user's computer under the control of a remote operator.

Prevention of Cyber Fraud

The Head of IT Support is responsible for and ensures that:

- firewalls and antivirus software are in place to protect the school network system and the systems are tested on a regular basis;
- data is backed up regularly;
- users are provided with the minimum level of access needed to do their jobs. When staff leave, their access is revoked immediately;
- staff are trained in checking that emails are genuine before sending passwords, information and bank details, and that any phishing emails are reported immediately to the ICT team;
- checks are carried out on all hardware and software and all configuration changes are authorised, documented and implemented. Only approved users can make changes. Software updates and security patches are implemented as soon as they are released;
- systems are monitored constantly, and any unusual activity is investigated.

Prevention of Fraud/Irregularity

The management and financial systems of the Trust have been designed to incorporate appropriate controls for preventing fraud. These controls include, inter alia:

- supervisory checks
- appropriate organisational structures
- complete, accurate and up-to-date records
- physical security of assets/stocks
- segregation of duties
- clearly defined written responsibilities
- clearly defined lines of reporting
- regulations and associated procedure guides
- audit investigations/reviews
- adherence to Financial Procedures
- discrete groups of Trust staff responsible for the certification of orders/payments etc.

Responsibility for Prevention

The CEO is ultimately responsible for the management of the Trust, including line management of the CFO and accountability arrangements. The CFO is responsible for ensuring that an adequate system of internal control exists within their areas of responsibility and that the controls operate effectively. The responsibility for the prevention and detection of fraud therefore rests, primarily, with the CFO, although all Trust staff are responsible for ensuring that fraud does not occur. There is a need for all managers to assess the types of risk involved with operations for which they are responsible, to review and test the control systems on a regular basis and to ensure compliance with control regimes.

In establishing effective internal controls, all managers should be aware of the following good practice concept:

- regular rotation of staff in 'control critical' functions
- wherever possible segregation of duties so that control of all aspects of the key function does not reside with one person e.g. bank details are not taken verbally and are checked by two different member of staff
- avoidance of processing backlogs
- considering the control implications whenever a new system is being introduced

A further check is provided by Auditors when carrying out an Extended Assurance visit when undertaking sampling checks as part of the role.

On line Banking

The preferred and regular method of payment is via electronic payment method, Bankers Automated Credit system (BACS) transfers, which is subject to stringent authorisation and control procedures:

a) the Finance Assistant prepares the BACs run report and checks that the appropriate supporting documentation is in place.
b) the Finance Manager carries out an initial review of the BACSs run report and supporting documentation.
c) the BACS run report is checked and signed in accordance with the Financial Procedures, prior to payment being made.

On line Banking passwords

Regular reminders from the bank prompt users to change on line banking passwords.

Credit Card

Robust procedures are in place to ensure proper use of the school's credit cards:

1) the school's credit cards are kept secure at all times in the safe;
2) credit card transactions are authorised by the budget holder;
3) the transaction is entered on to a control sheet immediately, so that any instances of fraudulent use can be identified;
4) usage of the card is spot checked by the Director of Business and Finance Manager;
5) the Finance Assistant ensures that all transactions on the credit card statement are supported by a VAT receipt if applicable;
6) if a credit card is lost, Lloyds Bank must be informed immediately. A 24 hour service is provided for this purpose. Telephone number: 0800 096 9779.

Caxton Card

Caxton cards are prepaid currency cards for use in the UK and overseas. The Trust has two Caxton cards. They provide a cash advance for staff on school trips to meet expenses. The "chip and PIN" process is a safe option for the Trust as it is an additional level of security. Sterling is loaded up in advance of the trip, and staff are required to account for all items of expenditure on the Caxton statement with supporting documentation and a summary of expenditure showing a breakdown of costs. VAT can be claimed for UK expenditure such as petrol as long as original documents are provided.

Action to take if a fraud or irregularity is suspected

If a member of staff suspects that an action or event, perpetrated either by another member of Trust staff or by a third party, may constitute a potential fraud or irregularity the suspicion should immediately be reported to his/her line manager. If the line manager of the member of staff reporting the case is implicated the suspicion should be reported to the next level of management. Management must ensure that the requirements of the Trust's Whistle Blowing Policy are fully met.

The line manager must then discuss the facts of the case with the person raising the issue. If the line manager considers that a fraud or irregularity may have occurred, or is likely to occur, he/she must immediately report the matter to the CFO, who must then report to the CEO, normally in writing, unless the CEO is implicated, in which case the Chair of Board of Trustees must be informed.

On receipt of the information the CFO or the CEO must arrange for an 'independent' member of the Trust management team or an auditor to undertake an investigation to establish the facts of the case. The investigation will usually include:

- informing the members of the Trust staff suspected of the fraud or irregularity and seeking his/her comments
- removing, for safe custody, any books, records or documents relating to the case
- confiscating any equipment relating to the case (e.g. personal computers, storage media, USB memory drives).

The protocols for conducting the investigation are to follow the usual Trust procedures and advice from the HR Advisor. The line manager concerned must also be consulted.

Where the investigation concludes that there is compelling evidence to suggest that fraud has taken place the following action is required:

Type of Fraud	Action
A. Sum involved is £0 to £1,000	1. Trust disciplinary procedure invoked 1. CFO or CEO reports case to: • the Chair of Board of Trustees

	• the CEO (unless the CEO is acting under section 4.3.2 above, or unless the CEO is under investigation) • the Audit and Risk Committee 2. CFO takes steps to recover any Trust property which has been unofficially removed from Trust premises. 3. The CFO or CEO will inform the police if there is evidence of a persistent fraud or a one off incident involving a loss of £50 or more.
B. Sum involved is £1,000 to £10,000	1. Trust Disciplinary Procedure invoked. 2. CFO or CEO reports case to: • the Chair of Board of Trustees • the CEO (unless the CEO is acting under section 4.3.2 above, or unless the CEO is under investigation) • The Chair of the Audit and Risk Committee • The Audit and Risk Committee • EFA, where £5000 and above 3. CFO or CEO • takes steps to recover any Trust property which has been unofficially removed from Trust premises • contacts solicitors and insurers, if appropriate • informs the police, addresses any questions of public relations or publicity
C. Significant fraud, usually where one or more of the following factors is involved: • in excess of £10,000; • the particulars of the fraud are unusual or complex; • there is likely to be great public interest because of the nature of the fraud or the people involved.	1. Trust Disciplinary Procedure invoked. 2. CFO or CEO reports case <u>without delay to:</u> • the Chair of Board of Trustees • the CEO (unless the CEO is acting under section 4.3.2 above, or unless the CEO is under investigation) • the Chair of the Audit and Risk Committee • the Trust Audit and Risk Committee, with a written report to the next Committee meeting CFO or CEO

	• takes steps to recover any Trust property which has been unofficially removed from the Trust premises • contacts solicitors and insurers, if appropriate • informs the police, addresses any questions of public relations or publicity

Advice should be sought from the HR Advisor in relation to the protocols for the actions listed in above.

Where the investigation concludes that there is compelling evidence to suggest that a fraud has taken place and it relates to the CEO, then the arrangements set out above apply, with the substitution of 'Chairman of Audit and Risk Committee' for 'CEO'.

If an allegation has been found to be groundless and it is believed that it has been made maliciously, the CEO may decide to discuss the allegation that the member of staff who first raised the issue concerned. The CEO may ask another member of Trust staff to do this on his/her behalf. The CEO may decide to invoke the Trust's Disciplinary Procedure in these circumstances.

Depending on the type and significance of the fraud, it may be appropriate for the Trust to submit a Suspicious Activity Report to the Serious Organised Crime Agency. The Audit and Risk Committee will determine when this is appropriate and, unless it decides otherwise, will delegate the submission of the report to the CFO

Learning from experience

Where a fraud or irregularity has occurred, Trust management will take steps to improve the controls in the systems where the fraud occurred. This will help to ensure that the fraud, or a version thereof, does not recur in the future.