One Community Trust

Anti-Fraud, Bribery and Corruption Policy

Author	**TR**
Approved by	**Trustees**
Approval Date	**07/12/2023**
Version Number	**4**
Status	**Approved**
Review Date	**Autumn term 2026**

CHANGE RECORD FORM

Version	Date of change	Date of release	Changed by	Reason for change
1	15/7/20	15/7/20	TR	Initial version
2	25/9/20	25/9/20	TR	Added ref to anti fraud & safe keys
3	20/05/2021	20/05/2021	TR	Updated re: Suppliers Form
4	19/11/23	06/02/24	TR	Updated ref to BRA committee

Fraud, bribery, corruption, or other dishonesty, would adversely affect the Trust's reputation and put at risk its ability to achieve its objectives by diverting resources from the provision of education for our pupils.

The purpose of this policy is to confirm the Trust's commitment to preventing and detecting fraud, bribery and corruption.

The Fraud Act 2006 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 created four new offences of:

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

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

"The international distortion of financial statements or other records by person internal or external to the organisation which is carried out to conceal the misappropriation if assets or otherwise for gain."

Fraud is different to theft, which is defined in the 1968 Theft Act as:

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

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 (Section 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 Trust 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 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."

The term "*fraud*" is used throughout this policy, for the purposes of this document the term also includes theft, bribery and corruption.

The Anti-fraud, Bribery and Corruption Policy applies to Trustees, Governors and all employees (full time, part time, temporary and casual) of the Trust and its academies.

Policy statement

The Trust expects all Trustees, Governors, Employees and those acting as its agents to conduct themselves in accordance with the 7 principles of public life defined by the Nolan Committee 1995. The 7 principles are:

- **Honesty**– holders of public office have a duty to declare any private interest relating to their public duties and to take steps to resolve any conflicts arising in a way that protects the public interest.
- **Integrity**– holders of public office should not place themselves under any financial or other obligation to outside individuals or organisations that might influence them in the performance of their official duties.
- **Selflessness**– holders of public officer should take decisions solely in terms of the public interest. They should not do so in order to gain financial or other materials benefits for themselves, their family, or their friends.
- **Objectivity**– in carrying out public business, including making public appointments, awarding contracts, or recommending individuals for rewards and benefits, holders of public office should make choices on merit.
- **Openness**– holders of public office should be as open as possible about all the decisions and actions that they take. They should give reasons for their decisions and restrict information only when the wider public interest clearly demands.
- **Accountability**– holders of public office are accountable for their decisions and actions to the public and must submit them to whatever scrutiny is appropriate to their office.
- **Leadership**– holders of public office should promote and support these principles by leadership and example.

Responsibility

The Trust aims to have in place efficient and effective systems of control that as far as possible prevent potential fraudsters from exploiting weaknesses.

Both Trustees and LGBs are responsible for ensuring there are strong and effective arrangements in place for managing the risk of fraud and ensuring the Trust's interests are safeguarded, including its reputation.

The risk is managed through the existence and application of appropriate policies and procedures. The wide range of procedures in place to minimise the risk of fraud constitute a major part of the system of internal control, which is designed to ensure the Trust conducts its business properly and effectively and completes its transactions fully, accurately and properly.

The Headteacher at each academy will advocate these policies and procedures and support strong action.

Key procedures and controls

The following key procedures and controls operate within the Trust:

- The Trust has an effective Anti-Fraud, Bribery and Corruption Policy and maintains a culture that will not tolerate fraud, bribery or corruption
- Trustees, Governors and employees comply with respective policies and procedures
- Risk Management procedures are in place

- A Register of Interests is maintained to enable Trustees, Governors and employees to record any financial or non-financial interests that may bring about conflict with the Trust's interests
- A Register of Gifts and Hospitality is maintained to enable Trustees, Governors and employees to record gifts and hospitality either received, or offered and declined, from contractors and suppliers
- Confidential Reporting (Whistleblowing) procedures are in place and operate effectively
- Suitable and enforced financial and contract procedures
- Robust recruitment and selection procedures
- Clear and active disciplinary arrangements
- Sanctions are pursued against those who commit fraud, bribery and corruption
- Staff attend fraud protection workshops wherever possible (see Appendix for latest guidance)
- Keys to school safes are removed from premises overnight

The Trust maintains a continuous overview of its arrangements for managing the risk of fraud. A regular review of the policy is carried out and the documents are reviewed as appropriate to reflect any key changes and to incorporate current best practice e.g. Trust will no longer accept change of bank details email. Supplier must complete OCT supplier change of bank details form.

The Trust expects that the individual and organisations with which it deals (e.g. partners, suppliers, contractors, and service providers) will act with integrity and without actions involving fraud, bribery and corruptions. Where relevant, the Trust will include appropriate clauses in its contracts about the consequences of fraud, bribery and corruption. Evidence of such acts is most likely to lead to a termination of the particular contract and will normally lead to prosecution.

In assessing the effectiveness of its arrangements, the trust will monitor the extent to which:

- Key personnel are trained in detecting and investigating fraud,
- Identified incidents are investigated,
- Perpetrators are robustly dealt with,
- The Trust responds to identified weaknesses in its systems and controls,
- There is any trend in incidents experienced,
- Perpetrators are prosecuted,
- Recovery of losses is sought.

Audit

The Business, Risk and Audit Committee and internal audit procedures are a key element of the Trust's control system. The internal audit function carries out a rolling program of audits as agreed by Trustees, designed to assess selected internal control systems. The external audit team provides an independent appraisal of the integrity of all-internal control systems.

Reporting fraud

The board of trustees must notify ESFA, as soon as possible, of any instances of fraud, theft and/or irregularity exceeding £5,000 individually, or £5,000 cumulatively in any financial year. Unusual or systematic fraud, regardless of value, must also be reported.

The following information is required:

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

Furthermore, all instances of fraud should be reported to Action Fraud at the National Fraud and Cyber Crime Reporting Centre using the following link:

https://www.actionfraud.police.uk/

Raising concerns

It is the responsibility of the Trustees, Governors, CEO, CFO, Headteachers and employees to prevent and help detect fraud, bribery and corruption. In high risk areas specific controls aimed at preventing and detecting frauds will be in place.

A decision will then be made as to who is best placed to investigate any concerns raised. The investigating officer also has the responsibility to report all findings to the Trust.

It is often the alertness of employees and the public that enables fraud to be detected. In accordance with the Whistleblowing Policy, any member of staff with any concerns about the Trust or its academies' activities should normally raise concerns through their immediate manager or the senior leadership team. However, it is recognised that this may not be possible in certain circumstances. In these cases, contact should be made with the Chair of Trustees, CEO or the CFO as appropriate. Concerns may also be raised with the Trust's External Auditor.

All concerns, reported by whatever method, will be treated in confidence and will be reviewed and investigated by the person deemed to be appropriate and best placed to do so. This may mean that, depending on the level, type and details of the concern raised, that concerns are investigated by the Trust, internal audit or in case of very serious concerns, the external auditor or the police.

Appendix A

Lloyds fraud protection webinar/Croft primary notes

A case study was demonstrated, whereby a person in finance received an email from her boss asking her to complete a payment providing bank details. They explained that it was urgent and that they would be busy all day on a conference call.

This person went ahead and made the payment trusting the instructions from their boss.

- Need to make sure processes are tight
- Raise awareness of scams
- Always verify an instruction using a different method of communication i.e. text/phone call, email not always tight
- Use strong passwords

Website ***haveibeenpwned.com*** – enter your email address and it tells you if your email has been compromised.

A strong password is essential. A 2 factor authentication plan i.e. details of mobile phone to send a text to.

Risk/fraud management at this vulnerable time with COVID and financial pressures.

- May receive phone calls from Government department, mention of tax rebates
- Office 365 VPN scam asking you to input details looks like Office 365 page
- COVID test, track and trace, asking for personal confidential details

Can staff be caught out?

When was the last time you had some training about phishing?

Verifying the payment process

- 2 forms of verification to communicate
- Payment approvers
- Make sure staff follow procedures when working remote
- Challenge process with new way of working

Open up channels of communication

- Look at spotting fraud activity among staff – method of monitoring
- Revoke access when they leave, return passes
- Technology – leavers process in place

Layered approach

- Technology other forms of communication to verify instructions
- Stringent and robust passwords – staff using applications

- Processes – embed new working from home procedures
- How do staff adhere to the processes
- Train and remind staff

Don’t just rely on email as single source of communication.

Dedicated pages on website:

- Lloydsbank.com
- Cyberaware.gov.uk

Mention any concerns to bank relationship manager.