Grove Learning Trust

Fraud, Bribery & Theft Policy

Ratified by Resources, Audit & Risk Committee
Summer 2025

Version Control

Version	Date	Status	Author (AU) / Approver (AP)
Draft 01	17/02/2021	Completion of first draft	PJB (AU)
Final – A	March 2021	Signed off by Trust Board	Trust Board (AP)
Final - B	March 2022	Signed off by Trust Board	Trust Board (AP)
Draft - 02	21/3/24	To be ratified by RAR Committee	LC (AU)
Final	10/6/24	Updated following feedback from RAR committee members	AG (AU)
Review	27/05/25	Review in line with policy schedule, changing job titles	DG (AU)
	June 25	Section titled: Links with other policies / documents and relevant documents listed	SR

Review

Next Review	Summer 2026

Contents

1. **Introduction** 4
2. **Rationale** 4
3. **Implications** 4
4. **Definitions and examples of fraud, bribery and theft** 5
5. **Responsibilities for preventing and dealing with fraud, bribery and theft** 5
6. **The 10 questions we must always be aware of** 7
7. **Cyber Crime** 8

1. Introduction

The following instruction sets out individuals' responsibilities for the prevention and reporting of incidences or suspicions of fraud, bribery and theft within the Trust and the procedures to be followed if it is suspected or discovered.

Employees must abide by the Trust's values and behaviours, which includes acting with honesty and integrity, and safeguarding the Trust's resources. It is everyone's responsibility, particularly line management, for detecting and dealing with fraud, bribery, and theft.

This instruction applies to all employees, contractors, and volunteers.

2. Rationale

The Trust's aim is to foster a culture where fraud, bribery and theft within our organisation is never acceptable and therefore we:

- Will put in place appropriate systems and procedures, incorporating efficient and effective internal controls, to prevent and detect fraud, bribery, and theft.
- Will investigate all reports of suspected fraud, bribery, or theft and where appropriate notify the police and seek to recover any losses.
- Believe that members of the public, employees, contractors, volunteers, and any other interested party should feel able to report any cases of malpractice or wrongdoing without fear of recrimination.
- Ask all employees to exercise proper stewardship of our charitable funds, and carry out all business fairly, honestly, and openly.

3. Implications

Fraud, bribery, or theft will usually result in direct financial loss but also presents a risk to our reputation and wider public trust in the organisation.

Grove Learning Trust considers actual or attempted fraud, bribery, or theft to be acts of gross misconduct and, if proven, may result in dismissal. Where supervisory negligence is found to be a contributory factor, disciplinary action may also be initiated against those managers/supervisors responsible.

Grove Learning Trust will always seek to recover any losses as a result of any acts of fraud or theft.

4. Definitions and examples of fraud, bribery, and theft

Fraud is the general term given to an act of deliberate deception with the intention of concealing the misappropriation of assets, any other personal gain or causing a financial loss to the Trust. Examples include:

- Falsification of claims, such as expenses, timesheets etc.
- Lying about qualifications on an application form or at interview.
- Intentionally overpaying suppliers for personal gain.
- Use of Grove Learning Trust equipment, property (including staff card) or services for personal gain.
- Making false claims and or the misuse of monies.
- Failing to disclose information which would influence a decision.
- Abuse of position to gain personal advantage for yourself or someone you know.
- Manipulation or misstatement of accounting records or results.

Bribery can either be described as:

- Active – offering or promising a bribe to influence someone's actions or to reward them for acting improperly; and
- Passive – the act of requesting, agreeing to receive, or accepting a bribe.

Theft is defined as when a person dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it.

5. Responsibilities for preventing and dealing with fraud, bribery and theft

Employees, contractors and volunteers

Employees, contractors, and volunteers must abide by the Trust's values and behaviours; this means:

- Safeguarding Trust resources.
- Ensuring the appropriate use of Trust resources. This includes cash and/or payment systems, use of petty cash, expenses claims, dealing with suppliers and use of Trust equipment.
- Declaring any potential conflicts of interest.
- Where possible, avoiding line management of partners or family members. If this is not possible, ensuring complete transparency by involving others in decision making processes relating to aspects of employment such as pay, benefits, access to training.
- Being vigilant for signs of fraud, bribery, or theft.
- Highlighting areas susceptible to the risk of fraud, bribery, or theft to management.
- Reporting suspicions of fraud, bribery or theft immediately using the Whistle-blowing Policy.

If an employee, contractor or volunteer suspect's fraud, bribery or theft is taking place they **must not** do the following:

- Alert the person(s) they suspect as this may enable them to cover their tracks.
- Discuss their suspicions or any related facts with anyone outside of the Trust unless specifically authorised to do so by their manager.
- Discuss their suspicions or any related facts with anyone within the Trust other than in accordance with this instruction or the whistle-blowing guidance.
- Attempt to investigate the matter themselves.

Line Managers
Where fraud, bribery or theft is suspected or detected it must be reported to the CFO who will work with the line manager to ensure that a full investigation is carried out and appropriate action is taken. This may include notifying the police and/or taking disciplinary action. If the line manager is personally involved or implicated in the case, this responsibility passes to their line manager; in the case of the Head of School, responsibility passes to the Executive Head Teacher, in the case of the Head Teacher, responsibility passes to the Deputy CEO.

The Board of Trustees must be advised of all cases of suspected fraud and may choose to engage the appointed auditors to investigate.

Internal Audit
Audit checks includes data matching exercises for the purposes of the prevention and detection of fraud. Data matching involves comparing computer records we hold for one purpose against other computer records held by the same for another purpose: for example, checking staff records against records of our suppliers to identify any potential conflicts of interest or fraudulent claims or payments.

An externally appointed auditor will be appointed to carry the internal audit function. The Trust has a rigorous internal scrutiny schedule which is carried out annually by a different external auditor company to the annual auditors, as instructed by the Board of Trustees.

Responsibilities of trustees and risk management strategy for managing fraud
The board of trustees must notify the ESFA, as soon as possible, of all instances of fraud, theft and/or irregularity exceeding £5,000 individually, or £5,000 cumulatively in any financial year.

Annex 4.9 of the HM Treasury publication Managing Public Money highlights the responsibilities and expectations of public sector organisations in relation to fraud.

An effective fraud risk management strategy involves:

- assessing your overall vulnerability to fraud
- testing your internal control system to ensure it is robust.
- identifying the area's most vulnerable to fraud risk, the list of potential fraud indicators may support this review
- evaluating the scale of fraud risk
- responding to the fraud risk through improved control arrangements
- measuring the effectiveness of the risk strategy to potential fraud
- reporting fraud

The most effective way to manage the risk of fraud is to prevent it from happening by developing an effective anti-fraud culture. Grove Learning Trust will discuss the anti-fraud strategy annually with trustees as part of reviewing any changes to the Academy Trust Handbook. The anti-fraud checklist for academy trusts is used to support this assessment.

The ten questions included in the checklist are intended to help the trustees, governors, accounting officers, CFO and finance staff to review their arrangements for preventing, detecting, and dealing with fraud should it occur. The risk of fraud is considered on an ongoing basis through the risk register, which is discussed at the Trust's RAR Committee, as is the schedule for internal audit; the annually updated financial procedures handbook; the delegated levels of authority and the overall compliance with the 'ESFA Academy Trust Handbook'.

A summary of the Handbook is discussed and circulated to all of the trustees, governors and Head Teachers / Head of schools in the Trust annually in September.

The 10 questions included in the checklist are:

1. Are trustees and the accounting officer aware of the risk of fraud and their responsibilities regarding fraud?
2. Is fraud included within the remit of the Trust's resources, audit and risk committee?
3. Has the role of the external auditor and responsible officer or equivalent regarding fraud been established and is it understood?
4. Is fraud risk considered within the Trust's risk management process?
5. Does the Trust have a fraud strategy or policy and is there a 'zero tolerance' culture to fraud in the Trust?
6. Is the strategy, policy and 'zero tolerance' culture promoted within the Trust, for example through financial regulations, disciplinary procedures, checks on new staff, induction process, staff training and the vetting of contractors?
7. Does the Trust have policies on whistleblowing, declaration of interests and the receipt of gifts and hospitality?
8. Does the Trust have appropriate segregation of duties?
9. Is it clear to whom suspicions of fraud in the Trust should be reported?
10. If there has been any fraud in the Trust, has a 'lessons learned' exercise been undertaken?

6. Cyber Crime

The Academy Trust Handbook states trusts must also be aware of the risk of cybercrime, put in place proportionate controls and take appropriate action where a cyber security incident has occurred.

Examples of cyber crime
Cyber-crime may involve malicious attacks on computer software including:

- Email hacking – gaining access to people's emails
- Phishing – messages that look like authentic sites asking for people's information
- Mal-advertising – using advertisements to download malicious code to your computer

Trusts must obtain permission from ESFA to pay any cyber ransom demands. ESFA supports the National Crime Agency's recommendation not to encourage, endorse, or condone the payment of ransom demands. Payment of ransoms has no guarantee of restoring access or services and is likely to result in repeat incidents.
Grove Learning Trust has insurance in place to protect against the risk of cyber-crime (Risk Protection Arrangement - RPA) and this requires certain conditions which must be to protect the Academy trust.

RPA Members must comply with the following conditions for cover to apply. In the event of a claim the Member will be required to evidence compliance with all of the conditions below:

1. All members must meet the Department for Education's Cyber security standard relating to backups. The standard states: "You should have at least 3 backup copies of important data, on at least 2 separate devices, at least 1 must be off-site."
2. All Employees or volunteers who have access to the Member's information technology system must undertake NCSC training annually. In the event of a claim the Member will be required to evidence that any Employee or volunteer involved in the claim has undertaken the NCSC training. This must be updated annually at the beginning of the academic year.
3. All Members must register with Police CyberAlarm: Registering will connect Members with their local police cyber protect team and in the majority of cases, a cyber-alarm software tool can be installed for free to monitor cyber activity. Where installed the tool will record traffic on the network without risk to personal data. https://www.cyberalarm.police.uk/
4. All Members must have a Cyber Response Plan in place. A template is available on the RPA Risk Management portal.

Grove Learning Trust will ensure it complies with the requirements of the RPA and Academy Trust Handbook and will review its cyber response plan at regular intervals.

To comply with the ESFA Academy Trust Handbook, the trust should as a minimum:

- Use firewalls, antivirus software and strong passwords
- Routinely back up data and restrict devices that are used to access data

Train all staff to ensure they:

- Check the sender of an email before they send data.
- Contact the sender by phone or in person, if an e-mail is sent requesting payment or change of payment details.
- Understand the risks of using public Wi-Fi
- Understand the risks of not following payment checks and control measures
- Undergo the National Cyber Security Centre (NCSC) training

Links with other policies / documents:

- Cyber Response Plan
- Finance Regulations Policy
- Code of Conduct – Staff
- Code of Conduct – Governance Team
- Gifts & Hospitality
- Whistleblowing