Eastwood Park Academy Trust (EPAT)

EPAT

Believe Succeed Together

Fraud Policy

Date Reviewed	June 2023
Date Ratified by the Trust	July 2023

Contents

1.0 Introduction

For the purposes of this policy, fraud is defined as 'dishonest, irregular or illegal acts, characterised by a deliberate intent at concealment or false representation, resulting in the diversion of resources, whether or not for personal gain, for the benefit of an individual or group of individuals at a consequent loss to the Trust'.

The objective of this policy is to safeguard the proper use of the Trust's finances and resources. The Trust derives most of its income from public funds and so has a particular responsibility to ensure that income and resources are used solely for the purposes intended.

Fraud is a serious matter and the Trust is committed to investigating all cases of suspected fraud. Any employee, regardless of their position or seniority, against whom prima facie evidence of fraud is found, will be subject to disciplinary procedures that may result in dismissal. The Trust will normally involve the police and may seek redress via civil proceedings.

This policy should be read in conjunction with the employee Code of Conduct Policy.

2.0 Prevention

2.1 Leadership

Members, Trustees, Local Governors and Senior Leaders, should ensure that their behaviour is demonstrably selfless and open, and should champion the Trust's policies on conflicts of interest, gifts and hospitality.

2.2 Policies

Fraud can be minimised through carefully designed and consistently operated management procedures. Members, Trustees, Local Governors and employees must comply with the Financial Regulations and Academy Trust Handbook and work within the confines of the Trust's finance-related policies and schemes of delegation.

2.3 Cash

Management of cash should include the following:

- Segregation of duties – a segregation of duties should help to prevent fraud.
- Reconciliation procedures – reconciliations should be reviewed by someone other than the person carrying out the reconciliation.
- Receipts should be issued in return for cash received, to provide an audit trail.
- Physical security, such as safe keys should be kept secure.
- Frequent banking.

2.4 Cheques

Cheques are often completed in ways which facilitate opportunist fraud. Cheques are sometimes intercepted by organised criminals who falsify payee and value details using sophisticated techniques. Debtors may also be told to make cheques payable to a private account, possibly using an account name which is similar to that of a constituent academy or the Trust.

The following preventative measures should be taken:

- Physical security - unused, completed and cancelled cheques should never be left unsecured. If cheques are destroyed a record of the serial numbers should be maintained.
- Frequent bank reconciliations - some frauds have gone undetected for long periods because accounts have not been reconciled promptly, or because discrepancies have not been fully investigated.
- Segregation of duties.
- Clear instructions to debtors about correct payee details and the address to which cheques should be sent. The address should normally be the accounts department, not the department which has provided the goods or services.
- Recording of all cash and cheques received.
- Use of electronic funds transfer (EFT) as an alternative to cheques.

2.5 Purchasing

Many of the largest frauds suffered by education institutions have targeted the purchase ledger. Preventative measures should be taken as follows:

- Segregation of duties.
- Secure management of the creditors' data.
- Requiring purchase orders for the procurement of all services, as well as goods.
- Matching the invoice amounts to the purchase order commitment.

Only reputable companies should be added to the list of authorised suppliers.

2.6 Fraud Checklist

The Trust should complete, at least annually, the Fraud Checklist to ensure all financial controls put in place are evaluated each year.

2.7 Cyber Security

Emails often host phishing attacks, scams or malicious software e.g. trojans and worms. To avoid virus infection or data theft, we instruct employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained e.g. “watch this video, it’s amazing”.
- Be suspicious of clickbait titles e.g. offering prizes, advice.
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or give-aways e.g. grammar mistakes, capital letters, excessive number of exclamation marks.

If an employee isn’t sure that an email they have received is safe, they should contact IT Support.

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure, so they will not be easily hacked, but they should also remain confidential.

Further information regarding password security can be found in the Trust’s Code of Conduct Policy.

3.0 Fraud Response Procedure

3.1 Initiating Action

Any stakeholder who suspect fraud or irregularity should report it as soon as possible to the Principal, or in the case of the Principal, the CEO, or in the case of the CEO, the Chair of the Trust.

Anyone suspecting fraud should cite the Trust's Whistle Blowing Policy, which provides protection against reprisal for any such disclosure.

3.2 Responsibility for Investigation

The Principal, or in the case of the Principal, the CEO, or in the case of the CEO, the Chair of the Trust will decide on the action to be taken. There will normally be an investigation led by an external auditor.

3.3 Prevention of Further Loss

Where the initial investigation provides reasonable grounds for suspecting an employee or others of fraud, the Principal, or in the case of the Principal, the CEO, or in the case of the CEO, the Chair of the Trust, will decide how to prevent further loss. This may require the suspension of the suspect or suspects, under the Disciplinary Misconduct Policy.

In these circumstances, the suspect or suspects should be approached, unannounced, and be supervised at all times before leaving the academy's premises. They should be allowed to collect personal property under supervision, but should not be able to remove any property belonging to the academy. Any security passes and keys to premises, offices and furniture should be returned.

The suspect's access to the academy will also be suspended, for example by changing locks, deactivating swipe cards and informing relevant staff not to admit the individual(s) to any part of the premises. Similarly, the Head of IT will be instructed to withdraw, without delay, access permissions to the academy's computer systems.

3.4 Establishing and Securing Evidence

The Trust will follow disciplinary procedures against any employee who has committed fraud and will normally pursue the prosecution of any such individual through the criminal courts.

The Principal, or in the case of the Principal, the CEO, or in the case of the CEO, the Chair of the Trust will:

- Ensure that evidence requirements are met during any fraud investigation.
- Establish and maintain contact with the police.
- Ensure that staff involved in fraud investigations are familiar with and follow rules on the admissibility of documentary and other evidence in criminal proceedings.

3.5 Reporting Lines

The Principal, or in the case of the Principal, the CEO, or in the case of the CEO, the Chair of the Trust will provide regular, confidential reports to the Trust which will include:

- Quantification of losses.
- Progress with recovery action.
- Progress with disciplinary action.
- Progress with criminal action.
- Estimate of resources required to conclude the investigation.
- Actions taken to prevent and detect similar incidents.

3.6 Notifying the Secretary of State

The Academy Trust Handbook includes a requirement that academies must notify the Secretary of State of any attempted, suspected or actual fraud or irregularity where the sums involved are, or potentially are, in excess of the amount set out in the funding letter. The Academies Handbook also states the Trust must notify the ESFA of instances of fraud, theft and/or irregularity exceeding £5,000 individually or £5,000 cumulatively in any academy financial year, as well as any unusual or systematic fraud, regardless of value.

3.7 Recovery of Losses

The Principal, or in the case of the Principal, the CEO, or in the case of the CEO, the Chair of the Trust, in conjunction with the Finance Officer and auditor, will endeavour to ensure that the amount of any loss is quantified. Repayment of losses will be sought in all cases. Where the loss is substantial, legal advice should be obtained about the need to freeze the suspect's assets through the court, pending conclusion of the investigation. Legal advice may be obtained about prospects for recovering losses through the civil court, where the perpetrator refuses repayment. The Trust will normally expect to recover costs in addition to losses.

3.8 Final Report

On completion of the investigation, a written report, normally prepared by the Principal, or in the case of the Principal, the CEO, or in the case of the CEO, the Chair of the Trust, shall be submitted to the Trust containing:

- A description of the incident, including the value of any loss, the people involved, and the means of perpetrating the fraud.
- The measures taken to prevent a recurrence.
- Any action needed to strengthen future responses to fraud, with a follow-up report on whether the actions have been taken.