

FRAUD POLICY AND FRAUD RESPONSE PLAN

Date of Last Review: January 2019

Date of Next Review: January 2022

Responsibility: Mr R. Carling

Advisory Body Signature: *R Carling*



1. POLICY STATEMENT

- 1.1 Education for the 21st Century (The Trust) is committed to the prevention of fraud and the promotion of an anti-fraud culture.
- 1.2 The Trust operates a zero-tolerance attitude to fraud and requires all of its Members, Trustees, governors, staff volunteers and independent contractors to act honestly and with integrity at all times, and to report all reasonable suspicions of fraud.
- 1.3 The Trust will investigate all allegations of actual, attempted or suspected fraud and will seek to recover any losses and pursue appropriate sanctions against the perpetrators. This may include criminal prosecution, disciplinary action, legal proceedings and professional sanctions.
- 1.4 This policy applies to all Members, Trustees, governors, staff (full time, part time, temporary and casual), consultants and volunteers.

2. DEFINITION OF FRAUD

- 2.1 For purposes of this policy, the definition of “fraud” is the same as that set out in the Fraud Act 2006. Thus, anyone working for E21C as a trustee, governor, member of staff or independent contractor would be committing fraud if he/she:
 - Makes a false representation dishonestly knowing that the representation was or might be untrue or misleading and with intent to make a gain for him/herself or another, to cause loss to the Trust or one of its schools, or expose either the Trust or a school to the risk of loss; or
 - Fails to disclose information to someone to whom he/she was under a legal duty to disclose that information and dishonestly intending, by that failure, to make a gain or cause a loss to the Trust or a school; or
 - Occupies a position in which he/she was expected to safeguard, or not to act against, the financial interests of the Trust or a school and abuses that position dishonestly intending by that abuse to make a gain/cause a loss
- 2.2 Detailed examples of fraud can be found in Appendix 1 but might include:

- Submitting (*or paying*) invoices for goods and services, knowing that they had not been ordered or received.
- Using the Trust's purchase card to make personal purchases.
- Intercepting a school payment and amending the name of the bank details, payee and/or the amount.
- Submitting false claims for sickness or expenses.
- Committing Cyber Fraud.

3. KEY RESPONSIBILITIES

3.1 The Trustees are responsible for overseeing the financial performance of the Trust and Trust schools, including its assets, making sure the Trust's money is well spent and measures are in place to prevent losses or misuse, including arrangements for preventing and detecting fraud.

3.2 They must, therefore, for example:

- Develop, implement and maintain adequate systems of internal control that prevent and detect fraud.
- Test the system of internal control and seek independent assurance when appropriate.
- Regularly review the Trust's anti-fraud policy (through the Finance and Audit Committee) and compliance with it to ensure it remains effective and relevant to the needs of the Trust and Trust schools.
- Ensure that the Trust's Finance and Audit Committee receive a report on compliance with this policy at least once each year.
- Ensure that all allegations of fraud are investigated rigorously, in compliance with relevant policies, procedures and legislation and commence disciplinary and/or legal action where appropriate.

3.3 Furthermore in conformity with the Academies Financial Handbook, the Trustees will:

- Notify ESFA of any instances of fraud, theft and/or irregularity exceeding £5,000 individually, or £5,000 cumulatively in an academy's financial year;
- Report any *unusual or systematic fraud* (e.g. regular occurrences of low value theft), regardless of value; and as required by paragraph 4.9.2 of the Handbook (2018), in doing
 - Provide the ESFA with:
 - full details of the event(s) with dates
 - the financial value of the loss
 - measures taken by the trust to prevent recurrence

- whether the matter was referred to the police (and if not, why)
- whether insurance cover or the risk protection arrangement has offset any loss

3.3 Governors and staff are responsible for:

- Familiarising themselves with the types of fraud that might affect the Trust and Trust schools.
- Ensuring they adhere to the agreed policies and procedures, thereby protecting the Trust and its schools' reputations and assets from fraud.
- Assisting in the investigation of suspected fraud when requested to do so, for example by providing witness statements.
- Familiarising themselves, and complying scrupulously with the Trust's Whistleblowing Policy which can be found on the Trust's website.

4. REPORTING SUSPISIONS

4.1 In order to ensure that the Trust can respond to Fraud promptly and effectively, where any Trustee, Governor or member of staff has reason to suspect that Fraud has occurred, he/she must report this immediately to the Chief Financial Officer (CFO), *who will then immediately notify the Chief Executive Officer (CEO) and Chair of Trustees (CoT), save that:*

- If the suspected fraud involves the CFO then the report should go to the Chief Executive Officer (CEO), who will then immediately notify the Chair of Trustees
- If the suspected fraud involves the CEO the report should go directly to the Chair of Trustees (CoT)
- If the suspected fraud involves the CoT then Charity Protect should be contacted (See Whistleblowing policy for details)

4.2 Under no circumstances should trustees, governors or members of staff attempt to investigate the matter themselves.

4.3 Furthermore to enable the Trust to prevent Fraud, a Trustee, Governor or member of staff should also report immediately to the CFO, CEO or Chair of Trustees any factors of which he/she becomes aware, which could increase the risk of Fraud occurring. Such factors might include, for example:

- The theft or loss of banking passwords, PINs or similar credentials; or
- Weaknesses in the arrangements for recording or securing cash which is held on Trust premises.

4.4 Anyone making a report under this section may rely on the provisions of

- The Trust's Whistleblowing policy; and those of
- The Public Interest Disclosure Act 1998 which protects employees who raise concerns about certain matters of public interest in good faith.

4.5 Staff can also obtain free independent advice from Charity Protect (formerly Public Concern at Work)

5. CONTACT DETAILS

Chief Financial Officer rcarling@e21c.co.uk
Chief Executive Officer cwhiting@e21c.co.uk
Chair of Trustees MarkWhitby@e21c.co.uk
Charity Protect www.pcaaw.org.uk. 0203 117 2520

6. FRAUD RESPONSE PLAN

The Trust has established guidelines on the immediate actions to be taken in the event of a fraud being discovered or suspected. They cover how and when to seek professional advice, securing evidence and preventing further losses (see Appendix 2).

Appendix 1

FURTHER EXAMPLES OF FRAUD

Below are some examples of the types of fraud that have affected Trusts and schools across the country.

Leases

Schools are often offered leases and rental or hire agreements for equipment such as photocopiers, phones and computers. Whilst technically schools have the freedom to sign operating leases, finance leases are not allowed.

Some of the deals look too good to be true with low or zero upfront costs, although they often entail high life time costs and severe exit penalties. These penalties can cost the same amount as the total amount of the lease.

Recruitment

Issues can arise if a senior member of staff recruits a family member or friend. By doing this a number of conflicts of interest can arise such as the senior member of staff signing off additional hours of work that have not been completed by a family member. There is also the possibility of the candidate not being the best person for the role.

If there is a potential conflict of interest, for example a family member has applied for a post within the Trust the member of staff concerned must disclose the potential conflict through the recruitment process. The Trust will ensure that appropriate

controls are put in place to manage the potential conflict in an open and transparent manner and the risk of impropriety is minimised.

Cheque Fraud

The use of cheques is minimal and reducing year on year but governors and staff should be aware of the possibility that cheques have been stolen from the cheque books and cashed or legitimate cheques have been intercepted and amended. Additionally, cheque amounts have been changed by the payee.

Some staff fail to line off after the payee's name on the cheque, which has resulted in the payee inserting an additional hundred before the actual amount. Cheque books are regularly checked and reconciled with payments that have been taken out of the Trust's account.

Purchase Cards

There are usage agreements that are in place to prevent the misuse of purchase cards. Again, purchase card transactions are regularly checked and reconciled.

BACS

BACS payments are not immune to fraud. There are a number of scams such as 'phishing' and 'vishing' which is where fraudsters attempt to obtain log in details by pretending to call from genuine high street banks. They often sound very professional and the fraudsters will sometimes ask staff to call them back on authentic sounding telephone numbers which the fraudsters have purchased to help them commit the fraud. Equally, it is important to ensure that BACS log in credentials are stored securely and not shared.

CEO/HT Fraud

CEO/HT fraud involves fraudsters posing as senior members of staff within the Trust. The fraudster spoofs or fakes an email so that it appears to have come from the CEO/Head Teacher's email address. The email will normally be sent to the school's finance or office staff and typically begin with a short informal sentence such as "Are you in the office?" Once the fraudster has managed to engage the school's staff they will ask for an urgent electronic payment to a supplier. The account details they provide are for accounts controlled by the fraudster. Schools must ensure that any urgent payment requests received by email or text are validated by telephoning or speaking to the CEO/Head Teacher in person.

Invoices

There have been instances where fraudulent invoices have been sent to schools for goods that haven't been ordered or received. Sometimes these invoices are for small amounts and sent out in their thousands to schools up and down the country. These

invoices are often sent during the holidays in the hope that staff will be too busy to check each invoice when they return for the start of term.

Income

It is common for schools to rent out their facilities in order to generate income. Fraud can occur when the income received, especially if payment is made in cash, is stolen by staff or third parties if not properly banked and/or secured.

Appendix 2

FRAUD RESPONSE LEAD

Where the CFO/CEO/Chair of Trustees receives a report under section 4 above he/she shall take the following steps:

A Appoint an Investigator

Appoint a person (if necessary from outside the Trust) of sufficient independence, expertise, and experience to investigate, and to report back to the Trustees as expeditiously as possible on the allegations; and take all steps necessary to ensure that he/she can have access to any documents, staff, and other resources which he/she reasonably requires in order to complete his/her investigation

B Secure Evidence

- i Take all steps which are necessary in order to gather, store and secure data evidence-which could be relevant to the investigation. These might include, for example:
 - Names, addresses, email addresses, telephone numbers and dates of birth.

- Descriptions (height, build, hair colour, ethnicity, clothing, distinctive features).
 - Dates and times of key events.
 - Vehicle registration numbers and descriptions.
 - Details of any conversations had or overheard.
 - Details of any actions or incidents that were observed.
 - Company and/or business details.
- ii Secure any physical evidence such as original invoices, receipts, letters, cheques and application forms. Try to minimise how many people and how often such evidence is handled. Fingerprint evidence can very quickly be destroyed.
- iii If any of the evidence is on a computer, immediately unplug the computer from its power source and remove it to a secure location. Don't attempt to shut the computer down through its operating system as this can alter or destroy key files and documents.
- iv NB
- Whilst initially securing the evidence it is important not to be tempted to begin a more substantial investigation, or accuse individuals directly, without seeking professional advice (see 'Seeking Advice' below).
 - If an investigation is undertaken without following the appropriate policies, procedures and legislation, or if individuals are accused without sufficient evidence, it may lead to the perpetrators avoiding a disciplinary, criminal or civil sanction.

C Seeking Advice

When an allegation of fraud is discovered it is important to seek professional advice as soon as possible. Advice can be sought from the CFO, CEO or Chair of Trustees. General advice about fraud is available from Action Fraud:

<http://www.actionfraud.org.uk/>

D Supporting Witnesses

Governors, members of staff and the public may be feeling vulnerable before, during and after they have brought an allegation of fraud to the attention of the Trust.

It is therefore essential to reassure witnesses that they have acted appropriately by raising their concerns. Members of staff should be aware of where they can find the Trust's **Whistleblowing Policy** and reminded that the

Trust does not tolerate reprisals, victimisation or harassment and will take all reasonable action to protect them.

In addition, the Trust will take steps to minimise any difficulties Governors or members of staff may experience as a result of raising a concern. For instance, if they are required to give evidence in criminal or disciplinary proceedings, the Trust will advise or arrange for them to receive advice and support about the process being followed.

