



Anti – Fraud Policy and Fraud Response Plan

Summer 2024





Anti- Fraud Policy and Fraud Response Plan

Summer 2024

Policy Statement

The Whinless Down Academy Trust is committed to the prevention of fraud and the promotion of an anti-fraud culture.

The Whinless Down Academy Trust operates a zero-tolerance attitude to fraud and requires all staff, trustees/governors and volunteers to act honestly and with integrity at all times, and to report all reasonable suspicions of fraud.

The Whinless Down Academy Trust will investigate all instances 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.

This policy applies to all staff (full time, part time, temporary and casual), consultants, volunteers, each school's Local Governing Body, Trustees and Members.

Definition of Fraud

The term 'fraud' is often used to describe complex financial offences such as false accounting. However, in its simplest form, fraud is lying. Some people will lie, or withhold information, or generally abuse their position to try to trick someone else into believing something that isn't true. Examples might include:

- Sending fake invoices for goods and services that weren't ordered or received.
- Use of the school's purchase card to make personal purchases.
- Intercepting a school cheque and amending the name of the payee and/or the amount.
- Submitting false claims for sickness or expenses.
- Email hacking/phishing

Individuals caught committing fraud can be prosecuted under the [Fraud Act 2006](#) if they make a false representation, fail to disclose information or abuse their position.

Further examples of the types of fraud that KCC are currently aware of are available on pages 7&8.

Key Responsibilities

The CEO is responsible for:

- Developing, implementing and maintaining adequate systems of internal control that prevent and detect fraud.
- Testing the system of internal control and seeking independent assurance when appropriate.
- Regularly reviewing the school's anti-fraud policy and compliance with it to ensure it remains effective and relevant to the needs of the school.
- Reporting compliance with the policy on at least an annual basis to the Trust Board.
- Reporting allegations of actual, attempted or suspected fraud to the Trust Board and the Trust **must** notify ESFA as soon as is operationally practical based on its particular circumstances, of any instances of fraud, theft and/or irregularity exceeding £5,000 individually or £5,000 cumulatively in any academy financial year. Any unusual or systematic fraud, regardless of value, **must** also be reported with the following information: 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 have offset any loss. (Academy Trust Handbook)
- Ensuring all allegations of fraud are investigated appropriately, in compliance with relevant policies, procedures and legislation and commencing disciplinary and/or legal action where appropriate.

The Trust Board are responsible for:

- Overseeing the financial performance of the schools, including its assets, making sure the school's money is well spent and measures are in place to prevent losses or misuse, including arrangements for preventing and detecting fraud.

Staff are responsible for:

- Familiarising themselves with the types of fraud that might affect the Multi Academy Trust, including their responsibility to protect against cyber crime through their use of school devices and email.
- Ensuring they adhere to the agreed policies and procedures, thereby protecting the Multi Academy Trust's reputation and assets from fraud.
- Reporting allegations of actual, attempted or suspected fraud to the CEO, and/or the Trust Business Manager, and/or the Trust Board.
- Assisting in the investigation of suspected fraud when requested to do so, for example by providing witness statements.

ESFA will not tolerate fraud. It reserves the right to conduct or commission its own investigation into actual or potential fraud, theft or irregularity in any academy trust, either as the result of a formal notification from the trust itself or as the result of other

information received. ESFA may involve other authorities, including the police, as appropriate. ESFA will publish reports about its investigations and about financial management and governance reviews at academy trusts in line with its own policy on publishing information. (Academy Trust Handbook)

Academy 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.

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.

To address the risk of fraud, theft and/or irregularity, education providers should as a minimum:

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

Education providers should also train staff to ensure that they:

- check the sender of an email is genuine before, for example, sending payment, data or passwords
- make direct contact with the sender (without using the reply function) where the email, for example, requests a payment or change of bank details
- if telephoning the sender to confirm authenticity, do not use the contact number within the email without first checking it is genuine
- understand the risks of using public Wi-Fi
- understand the risks of not following payment checks and measures

Reporting Suspicions

The Trust Business Manager, CEO, Trustees, Members and all staff are an important element of the school's stance on fraud and are required to raise any concerns that they may have. The CEO and Trust Board will deal with any financial irregularities robustly.

Staff should immediately report any concerns about actual, attempted or suspected fraud to the CEO. However, if the concerns relate to the CEO, staff should report their concerns to the Chair of Trustees.

Under no circumstances should staff investigate the matter themselves.

Should a member of staff, including the CEO and/or Trustees wish to seek advice about how to deal with an allegation of fraud, or want to report the matter anonymously, they can contact the ESFA

The Public Interest Disclosure Act 1998 protects employees who raise concerns about certain matters of public interest in good faith. Staff can obtain free independent advice

from the charity Public Concern at Work on **020 7404 6609** and find other helpful information at <http://www.pcaw.org.uk/>.

A copy of the academy's Whistleblowing Policy can be found on 'The SchoolBus' Policy Manager.

A referral form has been provided at Appendix 2 which may be used as a guide to the type of information that should be captured when an allegation of fraud arises.

Notifying the ESFA and External Auditor

The Academy Trust Handbook includes the requirement that:

"The Trust must notify the EFSA, as soon as is operationally practical based on its particular circumstances, of any instances of fraud, theft and/ or irregularity exceeding £5,000 individually, or £5,000 cumulatively in any academy financial year. Any unusual or systematic fraud, regardless of value, **must** also be reported."

The ESFA reserves the right to conduct or commission its own investigation into actual or potential fraud, theft or irregularity.

At an appropriate time, the CEO will notify the EFSA and/ or the Trust's External Auditors, where appropriate. They will also formally notify the Audit Committee (FSARC) and Trust Board.

Fraud Response Plan

Whinless Down Academy Trust has established guidelines for senior staff and the Trust Board on the immediate actions to be taken in the event of a fraud being discovered or suspected. It covers how and when to seek professional advice, securing evidence and preventing further losses (see Appendix 1).

Fraud Response Plan

It is important that allegations of actual, attempted and suspected fraud aren't ignored. Even seemingly insignificant concerns may later reveal a larger, previously unknown problem.

Securing Evidence

Ensure that any concerns are recorded fully. Whenever possible keep written notes that cover:

- Names, addresses 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.
- Telephone numbers
- Company and/or business details

Secure any physical evidence such as original invoices, receipts, emails, letters, cheques and application forms. Try to minimise how many people and how often evidence is handled. Fingerprint evidence can very quickly be destroyed.

If any of the evidence is on a computer, immediately unplug the computer from its power source. Don't attempt to shut the computer down through its operating system as this can alter or destroy key files and documents.

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.

Preventing Further Losses

It is important to minimise any additional losses. For example, if the allegations concern the theft or loss of banking passwords, PIN's or similar credentials notify the bank immediately.

Equally, if the losses relate to a weak process, for example cash is routinely kept unsecured in a drawer; ensure that the process is changed, at least temporarily, until more permanent and improved processes can be implemented.

Staff will also be trained on the role in preventing cyber security, with updates given when new guidance/advice is released.

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 Whinless Down Academy's Audit Team (FSARC), School's Financial Services, HR Connect, External Auditors, Legal Services and the Police. General advice about fraud is available from Action Fraud: <http://www.actionfraud.police.uk/>

You can contact WDAT Internal Audit Team as follows:

Tricia Sherling

Tsherling@stmartins.kent.sch.uk

You can also contact our External Auditors, Kreston Reeves:

Kimberley Foulkes

0330 124 1399

Kimberley.Foulkes@krestonreeves.com

Support for Witnesses

Members of staff, Governors/Trustees and the public may be feeling vulnerable before, during and after they have brought an allegation of fraud to the attention of the school.

Reassure witnesses that they have acted appropriately by raising their concerns. Members of staff should be provided with a copy of the **Whistleblowing Policy** and reminded that the Academy Trust does not tolerate reprisals, victimisation or harassment and will take all reasonable action to protect them.

In addition, the Academy Trust will take steps to minimise any difficulties 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 Academy Trust will advise or arrange for them to receive advice and support about the process being followed.

Examples of Fraud

Below are some examples of the types of fraud that have affected KCC and schools across Kent.

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 (see section 3

'Financing Major Purchases, KCC Loans, Salix Loans and Leases' of the Financial Controls guidance on KELSI). 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. One school fell victim to sharp sales tactics and ended up committing the school to 14 financial agreements for 12 photocopiers which resulted in expenditure of almost £900,000.

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 school, the member of staff concerned must disclose the potential conflict to the Headteacher, CEO or the Chair of Governors immediately. The Headteacher, CEO or Chair of Governors should 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

School cheque fraud has become an increasing problem within Kent, 10% of all cases referred to Internal Audit from April 2014 to January 2015 were a result of cheques being amended and forged. There have been instances where 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 should be regularly checked and reconciled with payments that have been taken out of the schools account.

Purchase Cards

There are usage agreements that are in place to prevent the misuse of purchase cards. However, there have been instances where members of staff have used the card for their own personal purchases. A recent investigation examined the use of a

purchase card that had been used for petrol, electrical goods, food, holidays and DIY. It transpired that both the Head Teacher and Office Manager had been extensively using the purchase card for their own personal use.

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 (such as 0845 223344) 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, and when members of staff leave their log in credentials must be deleted.

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.

CEO Impersonation Fraud

CEO fraud involves fraudsters posing as senior members of staff within the school, most often the Head Teacher. The fraudster spoofs or fakes an email so that it appears to have come from the 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 Head Teacher in person.

Fraud Reporting Form

If you have any concerns about fraud please contact Kelly Brown, CEO at ceo@whinlessdowntrust.co.uk or Alison Mackintosh, Chair of Trustees, at alisonm@prioryfields.kent.sch.uk

You do not need to give your name. All the information provided will be treated in confidence.

Name of the person(s) or organisation you suspect:

Address: (if known)

Place of work / department / job title: (If known)

Please provide details of your suspicions. You should include as much information as possible. For example, what was said in telephone or other conversations, dates, times and places, vehicles used, as well as the names of any other parties involved: (Continue on a separate page if necessary and attach any additional evidence you may have)

Your details: **(please leave blank if you wish to remain anonymous)**

Name:

Telephone number or contact address:

Please return this form in an envelope marked Private & Confidential to:
Kelly Brown, CEO. C/O Priory Fields School, Astor Avenue, Dover. Ct17 0FS.
or

Alison Mackintosh, Chair of The Whinless Down Academy Trust. C/O Priory Fields School, Astor Avenue, Dover. Ct17 0FS