Bishop Perowne
Church of England College
Endeavour Forever

ANTI-FRAUD POLICY

Who is responsible	**Chief Finance Officer**
Statutory Policy	**No**
Review timescale	**Annual or as required by Governors**
Review date	**January 2023**
Agreed by Governors at FGB	
Next Review Date	**January 2024**

Content

1. Introduction

1.1 Bishop Perowne C of E College requires staff at all times to act honestly and with integrity and to safeguard the public resources for which they are responsible. Fraud is an ever-present threat to those resources and therefore must be a concern to staff. The College will not accept any level of fraud and corruption; consequently, any case will be thoroughly investigated and dealt with appropriately.

1.2 The purpose of this policy is to set out the College's responsibilities regarding the prevention of fraud and the procedures to be followed where fraud is discovered or suspected. The college derives most of its income from public funds but also may receive charitable donations and income from parents. The college has a responsibility to ensure this income and resources are used solely for the purposes intended.

1.3 The college must adhere to the recommendations of the Academy Trust Handbook. This document states academies must be aware of the risk of fraud, theft and irregularity and address it by putting in place proportionate controls. Trusts must take appropriate action where fraud, theft or irregularity is suspected or identified.

1.4 The board of trustees must notify Education and Skills Funding Agency (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.

1.5 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.

1.6 ESFA may conduct or commission investigations into actual or potential fraud, theft or irregularity in any academy trust, either because of a notification from the trust itself or from other information received. ESFA may involve other authorities, including the police.

1.7 ESFA will publish reports about its investigations and about financial management and governance reviews at academy trusts.

1.8 ESFA also publishes guidance on reducing fraud. Trusts should refer to this and to the findings from ESFA's investigation reports, as part of its risk management approach.

2. Fraud, Corruption and Other Irregularity: Legal Meanings

2.1 The Fraud Act 2006 gives **fraud** a formal legal definition. The act defines a general offence of fraud which is divided into three categories:

- **Fraud by false representation**: this is where a representation is made dishonestly, and with the intention of making a gain or causing a loss or risk of loss to another. A representation is defined as false if it is untrue or misleading and the person making it knows that it is, or might be, untrue or misleading. Representation can be stated by words or communicated by conduct, i.e. in written, spoken or electronic form;

- **Fraud by failing to disclose information**: this covers situations where a person fails to declare information which he/she has a legal duty to disclose. A person acts dishonestly and intends to make a gain, cause a loss to another or expose another to a risk of loss; and

- **Fraud by abuse of position**: this is where a person in a privileged position acts dishonestly by abusing the position held; and by doing so, fails to disclose to another person, information which he/she is legally required to disclose. The dishonest act is carried out with the intention of making a gain, or with the intention of causing a loss or risk of loss to another. The offence may be committed by omitting to make a declaration as well as by an act.

2.2 The introduction of the Fraud Act 2006 does not prevent the prosecution of offences under the various Theft Acts and the Forgery and Counterfeiting Act, such as theft, counterfeiting and falsification of documents.

2.3 **Corruption** is a specific type of fraud and involves the offering, giving, soliciting or acceptance of any inducement or reward which may influence the action of any person. Corruption involves two or more people. It does not always result in a loss; indeed the corrupt person may not benefit directly from his/her actions.

2.4 An **irregularity** may arise in connection with any significant matter or issue, other than fraud or corruption. For example, it may be caused by a member of staff who makes a genuine error or mistake in the course of his/her duties, but where this error or mistake is subsequently hidden from the College, perhaps to its ongoing detriment. An irregularity may also involve consideration of the possible inappropriate use of College funds or assets, but which may not technically constitute fraud or corruption.

2.5 For the sake of simplicity, this policy groups the legal concepts of fraud, corruption and irregularity under the single word “fraud.” References to fraud in the subsequent sections of this policy shall be taken to include instances of corruption and irregularity.

2.6 Please see appendix 1 for the type of fraud the college could be susceptible to and indicators of preventative measures put in place to mitigate risks.

3. Cybercrime

3.1 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.

3.2 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

3.3 As part of the Department For Education Risk Protection Arrangement that Academies can sign up to for Insurance Cover Cybercrime is covered however a caveat of tis is that schools obtain Cyber Essentials Certification.

3.4 The college was part of a pilot scheme in 2021-22 and received free insurance after obtaining Cyber Essentials Certification and the college is currently renewing this certification for 2-22-23.

4. The College’s Responsibilities

4.1 Overall responsibility for dealing with fraud and corruption rests with the Head Teacher as the College’s Accounting Officer.

4.2 As the College’s Accounting Officer, the Head Teacher’s responsibilities include:

- Establishing and maintaining a sound system of internal control to prevent fraud;
- Establishing effective financial regulations, policies and procedures;
- Establishing appropriate mechanisms for reporting fraud risk issues including reporting to the Trustees and the ESFA where appropriate;
- Ensuring that vigorous and prompt investigations are carried out;

- Taking appropriate legal and/or disciplinary action where fraud is proven;
- Ensuring that appropriate action is taken to minimise the risk of similar frauds in the future; and
- Taking appropriate action to recover assets and minimise the loss.

4.3 The Trustees are responsible for:

- Overseeing the financial performance of the school, including its assets, making sure the school's money is well spent and that measures are in place to prevent losses or misuse, including arrangements for preventing and detecting fraud;
- Seeing that the system of internal control is tested 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;
- Reviewing compliance with the policy on at least an annual basis;
- Reviewing all allegations of actual, attempted or suspected fraud and ensuring that matters are referred to the police if the Governing Body believes there are serious grounds for suspicion; and
- 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.

Please refer to the Finance Policy of the college for specific details on systems of internal control in place to safeguard the assets the college and their management of public funds.

4.4 Trustees and staff in positions of financial responsibility and authorisation are required to disclose information concerning their direct or indirect pecuniary interests, and those of close family members, via the Annual Declaration of Interest Form and to keep that information up to date. The Clerk of the Trustees is responsible for maintaining an up-to-date file of these forms. More details of these responsibilities are outlined in the college's Finance Policy.

5. Line Management Responsibility

5.1 Line managers are responsible for ensuring that an adequate system of internal control exists within their areas of responsibility and that those controls are effective. The responsibility for the prevention and detection of fraud therefore, rests primarily with line managers. There is a need for all line managers to assess the types of risk that their individual teaching department or support function is exposed to; to review and test those control systems regularly; to ensure that controls are being complied with; and to satisfy themselves that their systems continue to operate effectively.

5.2 Line managers must be alert to the possibility that unusual events or transactions could be symptoms of fraud or attempted fraud. Fraud may also be highlighted as a result of specific management checks or be brought to management's attention by a third party.

5.3 The Chief Finance Officer (CFO), whose remit includes direction of the College's finance function, acts as the Head Teacher's primary source of advice and assistance on anti-fraud control issues. The CFO is responsible for providing an opinion to the Head Teacher on the adequacy of arrangements for managing the risk of fraud and assisting in the deterrence and prevention of fraud by examining and evaluating the effectiveness of controls. In terms of establishing and maintaining effective controls, it is generally desirable that when new systems are being designed, safeguards against fraud are considered at an early stage.

6. Staff Responsibilities

6.1 It is the responsibility of all members of staff within at the College to ensure that public funds controlled by the College are safeguarded against fraud. Staff must alert their line manager if they believe an opportunity for fraud exists because of poor procedures or controls. Staff must report any suspicion of fraud immediately to their line manager (or other person in authority where appropriate) who should record this and report it to the CFO or, in the event that allegations of malpractice are made against the CFO, to the Chair of the Trustees. Members of staff are required to co-operate fully with any internal checks, reviews or fraud investigations. All members of staff are required to comply with the College's anti-fraud policies and procedures. Failure to comply may result in disciplinary action.

6.2 All members of staff have the right to "blow the whistle" on what they perceive to be a cause of serious concern or malpractice. All staff should familiarise themselves with the College's whistleblowing policy and the protection afforded them under the Public Disclosure Act 1998. The board of trustees assures all staff that they will not suffer in any way as a result of reporting reasonably held suspicions. A copy of the school's Whistleblowing Policy can be found on the school's website bishopperowne.co.uk or can be obtained from the head teachers personal assistant, Karen Wigley.

6.3 In devising and implementing its anti-fraud policy, the College subscribes to the **seven principles of public life** set out in the Nolan Committee's first report, *Standards in Public Life*. All College staff and members of the Governing Body are expected to uphold and reflect these principles to the greatest extent possible. The seven principles are as follows:

- **Selflessness**: holders of public office should take decisions solely in terms of the public interest. They should not do so in order to gain financial or other material benefits for themselves, their family, or their friends.

- **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.

- **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.

- **Accountability**: holders of public office are accountable for their decisions and actions to the public and must submit themselves to whatever scrutiny is appropriate to their office.

- **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.

- **Honesty**: holders of public office have a duty to declare any private interests relating to their public duties and to take steps to resolve any conflicts arising in a way that protects the public interest.

- **Leadership**: holders of public office should promote and support these principles by leadership and example.

7. Fraud Response Plan

7.1 The College would follow its disciplinary procedures and potentially involve, where necessary and appropriate:

- The Board of Trustees;

- The ESFA;

- The College's External Auditors; and

- The Police.

8. Creating an Anti-Fraud Culture

8.1 The creation of an anti-fraud culture underpins all other work to counter fraud. College staff must understand the risk of fraud, that fraud is serious and that it has the potential to divert valuable resources from the College's primary objective. The College recognises the importance of training in the delivery of high quality services and the College supports the principle of fraud awareness training for key staff involved with internal control systems who in the opinion of the Head Teacher and/or the CFO would benefit from such training.

9. Detection and Investigation

9.1 Where a fraud is detected or suspected, initial responsibility for investigating the matter rests with the CFO who has been nominated as the College's Investigating Officer. In his absence, or if the CFO is in any way alleged to be involved in the fraud, responsibility for investigating the matter rests with the Chair of the Trustees or in her absence one of the other trustees. The Investigating Officer shall inform and consult with the Head Teacher in all cases except where the Head Teacher is the alleged perpetrator. Investigations will be commenced as soon as possible.

9.2 If it is suspected that a significant or complex fraud may have occurred then a comprehensive investigation must be carried out by an experienced fraud specialist or the case must be referred to the police.

9.3 It is essential that all material that may be of evidential value must be recovered and preserved for further investigation if required. Additionally, the College must consider whether to suspend any individual who is the subject of the investigation, under the College's disciplinary procedures. Suspension is a neutral act; it may be necessary to safeguard further evidence that may be used to prove or disprove the allegation. Suspension is with pay where there is no acceptable or workable alternative, such as removal from normal duties or the imposition of restrictions to avoid future risks

10. Sanction and Redress

10.1 The College's disciplinary procedures provide for offences such as fraud, theft and deliberate falsification of registers, reports, accounts, expense claims and self-certification forms to be regarded as gross misconduct which may result in dismissal. The College will take disciplinary action in all cases where it is considered appropriate.

10.2 In cases where fraud is proven the College will notify the police of the outcome. The College will co-operate fully with the investigating body and will always seek to recover funds lost through fraud. It may be necessary for the College to initiate a Civil Action against the fraudster(s). If, during the investigation any failure of supervision is identified, the Academy must consider whether disciplinary action is appropriate for those involved.

11. Learning from the Experience

11.1 Where fraud has occurred it is vital that the Trustees, the Head Teacher and the CFO recognise the need to examine systems and procedures and make necessary changes to ensure that similar frauds will not occur. In addition to an internal control and scrutiny review advice would be sought from outside bodies, e.g. the College's auditors, the ESFA and peers in other academies, in respect of changes to systems and procedures.

12. Conclusion

Whilst the circumstances of fraud will undoubtedly vary, it is important that each individual case is subjected to the same rigorous process of investigation and redress. The College values the contributions made by its dedicated and loyal members of staff and governors, but the College wishes to reiterate that it views fraud very seriously and will not hesitate to take appropriate action in every case.

13. Review of Fraud Policy

13.1 The Anti-fraud Policy will be reviewed annually to ensure it is fit for purpose. It will be shared with the Trustees as necessary to ensure the College is taking account of all changes in types of fraud, government advice and recommendations of the Academy Trust Handbook to assure them that all assets of the College have the best protection against fraud. It should consider the policy in line with the college's policy for financial and internal control.

Appendix 1: Examples of School-related Fraud

Please see below for the types of fraud that could affect the college

Cyber Crime and Cyber security

In the digital age we live in this is increasingly an area where criminals and fraudsters are targeting organisations. Cyber-crime is criminal activity committed using computers and/or the internet. It can involve malicious attacks on computer software, including:

1. **Email hacking**

- Email hackers try to gain access to email accounts by tricking people to:
- open and respond to spam emails
- open emails with a virus
- open phishing emails

2. **Phishing**

- Phishing messages look authentic with corporate logos and a similar format to official emails.
- Sometimes phishing emails use the title of a genuine email that the victim has recently replied to in order to trick the victim into believing the communication is authentic. Phishing emails can appear to have originated from within or outside your organisation.
- Unlike official communications, phishing emails ask for verification of personal information, such as account numbers, passwords or date of birth.
- Sometimes the emails suggest the request is time sensitive to pressure the recipient to respond when they might not otherwise have done so.
- Unsuspecting victims who respond may suffer stolen accounts, financial loss and identify theft.

3. **Malvertising**

- Malvertising can compromise computers by downloading malicious code when people hover on or click on what looks like an advert. Some will even download malicious code to your computer while the website is still loading in the background. Cyber criminals can use advertisements to hack into computers.

Prevention

- Use firewalls, antivirus software and strong passwords
- Routinely back up data and restrict devices that are used to access
- Ensuring there is adequate network and malware protection
- Providing regular training to all staff and include as part of any staff induction
- Setting clear policies on mobile working and the use of mobile media
- Including regular review of policies as part of the risk management policy
- Specifically encouraging and reminding staff to:
  - 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
  - to regularly change passwords and not write them down where they can be easily accessed
  - adhere to the school's policies on the general protection of data (GDPR)

Please note the school undertook a Cyber Essentials Assessment to ensure that the school had good internal control to prevent fraud and have received Certification and free insurance through he Risk Protection Arrangement for insurance from ESFA. It is recommended this be reviewed as pat of the ICT Policy with the schools ICT Support Partner.

Cheque Fraud

Cheques can be stolen and cashed or intercepted and amended. Key measures to mitigate include:

- Physical security - unused, completed and cancelled cheques should never be left unsecured. Spoiled cheques should not be destroyed but should be clearly marked 'VOID' and lines marked through the print. They should then be filed along with the relevant documentation for future reference. Cheque books to be kept in a locked cupboard or safe
- Frequent bank reconciliations which are signed off by the Head Teacher- 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 between the entering of transactions and monitoring
- 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.
- Central opening of all post by and recording of all cash and cheques received.
- Use of electronic funds transfer (such as BACS) as an alternative to cheques.

Purchase, Debit or Charge Cards

There have been instances where members of a schools staff have used the school's bank card for their own personal purchases. Prevention of fraudulent use can be provided by:

- Limiting the use to specific staff
- Segregation of duties in person using the card and the person checking and reconciling the card statement
- Reconciling of statement and purchases on a monthly basis
- Adhering to finance policy on purchases as with any other transaction

BACS Payments

Fraudsters have attempted to obtain a school's bank log-in details by pretending to call from genuine high street banks. The fraudsters have often sounded professional and have sometimes asked 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. Always cheque directly with the bank and their relationship team before giving any information away.

Payment of Fraudulent Invoices

Receipt of invoices for goods that have not been ordered or received. If by email, cheque sender details as above. Ensuring Finance Policy on authorisations and ordering are adhered to. Ensuring a supplier list for regular approved suppliers is available and adhering to the Finance Policy for setting up and vetting any potential/new suppliers.

Rent Income

Fraud has occurred when the income received, especially where payment is made in cash, is stolen by staff or third parties if not properly banked and/or secured.

Lettees should be encouraged to pay by BACS or standing order only. If any cash is received it should be checked by two authorised personnel.

Equipment Leases

Schools have been offered leases or rental agreements for equipment such as photocopiers and computers. The terms of such agreements have been punitive with high lifetime costs and severe exit

penalties, amounting to sharp practice. Schools should adhere to the Academy Trust Handbook on leases and if in any doubt consult with their external auditors.

Recruitment and Overtime

Potential new members of staff must be screened before appointment, particularly for posts with financial responsibility.

References should cover a reasonable, continuous period of at least three working years, and any gaps should be explained.

An official employer's reference should be obtained.

Doubts about the contents of the reference should be resolved before confirming the appointment. If this is done by telephone, a written record of the discussion should be kept.

Where possible, qualifications should be checked before making an offer of employment, for example by requiring original certificates at the interview.

Checks should be undertaken e.g. Enhanced Disclosure & Barring Service with barred list information.

Checks should be undertaken to verify that candidates for teaching posts are not prohibited from teaching

Any overtime should be signed off by a line manager before it is actioned.

ESFA Guidance please see attached links for further information:

https://www.gov.uk/government/publications/indicators-of-potential-fraud-learning-institutions/indicators-for-potential-fraud-a-generic-checklist-for-education-providers

https://www.gov.uk/government/publications/indicators-of-potential-fraud-learning-institutions/guide-on-cyber-crime-and-cyber-security-for-education-providers

https://www.gov.uk/guidance/academies-guide-to-reducing-any-risk-of-financial-irregularities

https://www.ncsc.gov.uk/section/education-skills/cyber-security-schools

https://www.ncsc.gov.uk/files/NCSC-Alert-Further-targeted-ransomware-attacks-education-sector-March-2021.pdf