Barton Peveril Sixth Form College

ANTI FRAUD POLICY

Updated by	Vice Principal (Business Services)
Approved by	Corporation
Approval date	July 2026
Next review date	June 2029

1. INTRODUCTION

1.1. This document details the College's policy towards detected or suspected acts of fraud, bribery or other irregularity, whether relating to employees, Governors and/or External Members, students, suppliers, contractors, sub- contractors, partners or any other related third party.

1.2. The College receives the majority of its funding from public funds and one of the basic principles governing its actions is the proper use of public money.

1.3. The policy will be made available to all staff via the College Intranet as well as the Gifts and Hospitality and Anti-Bribery Policies, and in doing so, all staff should make themselves aware of these policies and their consequences, in order that they conduct themselves in an appropriate manner.

1.4. The purpose of this policy document is to set out responsibilities with regard to fraud prevention, what to do in the event of a suspected fraud and the action that will be taken by management.

1.5. The Corporation is committed to maintaining an accountable, honest, open and well-intentioned ethos in the College. All staff and students can be confident that they will not be victimised as a result of reporting a reasonably held suspicion of fraud or corruption. Victimising or deterring someone from reporting concerns is a serious disciplinary matter and should be reported to the Principal or Chair of Corporation. Malicious unfounded allegations will also be regarded as a disciplinary matter.

2. DEFINITION OF FRAUD

What is Fraud? - Fraud is defined in the Fraud Act 2006 and includes fraud by false representation, fraud by failing to disclose information and fraud by abuse of position, as detailed below:-

Fraud by false representation

Which may be expressed or implied. A person commits fraud by false representation if they:

Dishonestly make a false presentation with the intention:
- To make a gain for himself of another, or
- To cause loss to another or to expose another to a risk of loss.

A representation is false if:
- It is untrue or misleading, and
- The person making it knows that it is, or might be, untrue or misleading.

Fraud by failing to disclose information

A person commits fraud by failing to disclose information if they:

Dishonestly fail to disclose to another person information which they are under a legal duty to disclose, and;

Intend, by failing to disclose the information:
To make a gain, either for himself or for another, or
To cause loss to another or to expose another to a risk of loss.

Fraud by abuse of position

A person commits fraud by abuse of position if they:

Occupy a position in which they are expected to safeguard, or not to act against, the financial interests of another person, and

Dishonestly abuse that position, and

Intend, by means of the abuse of that position to
Make a gain for himself or another, or
Cause loss to another or to expose another to a risk of loss.

A person may be regarded as having abused their position either through an omission or by a specific act.

A ‘gain’ means a gain in money or other property, either temporary or permanent, and can include ‘keeping what one has’, as well as ‘getting what one does not have’.

Computer fraud is where information technology equipment has been used to manipulate programmes or data dishonestly (for example, by altering, substituting or destroying records, or creating spurious records), or where the use of an IT system was a material factor in the perpetration of fraud. Theft or fraudulent use of computer time and resources, including unauthorised personal browsing on the internet, is included in this definition.

3. RESPONSIBILITIES

3.1. The primary responsibility for prevention and detection of fraud rests with those charged with governance and management.

3.2. The Senior Leadership Team and the Governing Body are responsible for:

- Developing and maintaining effective, efficient and visible procedures and controls to prevent and minimise the risk of fraud and bribery e.g. College Financial Regulations.
- Producing a clearly defined and publicised Anti-Fraud & Bribery Policies which apply to everyone in, or involved with, the College and encourages open reporting of concerns.

- Ensuring that all staff, and Governors are aware of their duties and the required standards of conduct.
- Ensuring that all relationships with third parties (students, suppliers, contractors, sub-contractors, partners or any other related third party) are conducted on a basis that is compliant with the provisions of the Bribery Act 2010.
- Protecting and supporting against harassment or victimisation, those who, in good faith, make allegations of suspected irregularities.
- Safeguarding the rights of any persons subject to investigation.
- Carrying out vigorous and prompt investigations if suspicion of an act of fraud, bribery or other irregularity arises.
- Taking or instigating appropriate legal and/or disciplinary action against perpetrators of fraud or bribery and taking disciplinary action against managers where supervisory failures have contributed to the breach.
- Reporting the outcome of any such investigations to the appropriate officers and authorities.

3.3. The Audit Committee reporting to the Governing Body should ensure that its Terms of Reference in relation to fraud are strictly adhered to and that requirements under the Post-16 Audit Code of Practice are followed should such a situation arise.

3.4. The College's External Auditors are responsible for obtaining reasonable assurance that the Financial Statements are free from material misstatement including those caused by fraud. Two types of fraudulent misstatement are relevant to auditors i.e. fraudulent financial reporting and misappropriation of assets.

3.5. The Senior Leadership Team, advised by its Internal Auditors, is responsible for:

- Identifying the risks within systems and procedures.
- Developing and maintaining effective controls to prevent and detect fraud or acts of bribery.
- Ensuring that policies and controls are regularly reviewed, updated and complied with.

3.6. The Vice Principal (Finance & Resources) is the named officer responsible for fraud prevention. He/she is responsible for carrying out a risk assessment of fraud and bribery risks within the College and reporting these to the Senior Leadership Team.

3.7. College staff are responsible for acting with propriety in all College activities and this includes:

- The handling and use of any funds, monies, stock or any other consumables or assets (including scrap), that have a value.

- Dealings with students, Governors, contractors or suppliers, sub-contractors or partners or any other aspect of College business.
- Ensuring that they do not request, accept, or agree to receive, gifts, hospitality or benefits of any kind from any third party which might be seen to compromise their personal judgement or integrity or infringe the Bribery Act 2010. Employees should refer to the College's Gifts & Hospitality Policy for further information.
- Ensuring that they do not offer, promise or give any form of bribe to obtain or retain business.
- Communicating their concerns as appropriate.
- Adhering to all relevant College policies regarding confidentiality and any other relevant regulations, protocols and procedures regarding their behaviour and conduct.
- Ensuring that claims for personal expenses are compiled with integrity.
- Cooperating fully with any investigation covered by this policy, whether conducted by College Managers, Internal Auditors, the Police or other Authority.

4. CYBER FRAUD

4.1. Fraud can be, and increasingly is being, carried out using computers. Misuse of computers and their programs (i.e. software) are specifically covered by the Computer Misuse Act 1990.

4.2. A person is guilty of such an offence if, with intent, they access any program or data held on a computer which they are not authorised to access and / or they cause unauthorised modification to the contents of the computer such that the operation or access to the computer or program is hindered. Unauthorised disclosure of any personal data held on computers may also result in an offence under the Data Protection Act 2018 - which is the UK's implementation of the General Data Protection Regulations (GDPR).

4.3. The most common cyber problems are identified as

- Malware (virus / spyware)

- Phishing (fraud)

  The simplest to initiate, is an unauthorised change of supplier bank details where notification is received requesting a change of bank account details for creditor payments. Upon receipt of such a request the College is to:

  Verify with the supplier, using previously held contact data, the validity of the request

  Obtain email confirmation from supplier

  Automated accounts software to be updated by a Finance Officer who IS NOT a cheque signatory.

Periodically, at least monthly, the Finance Manager is to run and check an audit report showing changes to bank account data.

- Phishing (Impersonation)
  Where a seemingly genuine email from a senior executive instructs the recipient to make an immediate or emergency payment. Upon such a request the College is to:
  Take no action if the email is readily identified as spurious
  If in doubt the recipient is to make contact either by telephone or in person with the senior executive
  Report the incident to the Vice Principal (Finance and Resources)

- Website hacked/defaced

- Personal data theft

- Ransomware (encrypting malware)

4.4. At a minimum, staff should take the following steps to avoid on-line fraud:

- Ensure that usernames and passwords are unique
- Never share username or password with another member of staff
- Do not respond to, open an attachment in, or click on a link within an email if the message is suspected as fraudulent
- Never respond to emails requesting personal data, bank accounts, passwords etc.
- Never leave your computer unattended whilst logged on.

5. FRAUD RESPONSE PLAN

5.1. Introduction

5.1.1. This fraud response plan provides a checklist of actions and a guide to follow in the event that fraud is suspected. It covers:

Notifying suspected fraud
The investigation process
Liaison with police and external audit
Initiation of recovery action
Reporting process
Communication with Funding Bodies

5.1.2. Its purpose is to define authority levels, responsibilities for action and reporting lines in the event of suspected fraud, theft or other irregularity.

5.2. Notifying Suspected Fraud

5.2.1. It is important that all staff are able to report their concerns without fear of reprisal or victimisation and are aware of the means to do so. The Public Interest Disclosure Act 1998 (the "whistle-blowers Act") provides appropriate protection for those who voice genuine and legitimate concerns through the proper channels. (See the College's Whistleblowing Policy)

5.2.2. In the first instance, any suspicion of fraud, theft or other irregularity should be reported, as a matter of urgency, to your line manager. If such an action would be inappropriate, your concerns should be reported upwards to one of the following people:

- Director of Department or Support Staff Manager
- Member of Senior Leadership Team
- Chair of Corporation (via Clerk to Corporation)

5.2.3. Members of staff may wish to contact the College's internal auditors for advice if they have concerns. The Clerk to the Corporation can provide contact details for the auditors' hotline.

5.2.4. Every effort will be made to protect an informant's anonymity if requested. However the College will always encourage individuals to be identified to add more validity to the accusations and allow further investigations to be more effective. In certain circumstances, if anonymity cannot be maintained, this will be advised to the informant prior to release of information.

5.3. The Investigation Process

5.3.1. Suspected fraud must be investigated in an independent, open-minded and professional manner with the aim of protecting the interests of both the College and suspected individual(s). Suspicion must not be seen as guilt to be proven.

5.3.2. The investigation process will vary according to the circumstances of each case and will be determined by the Principal in consultation with the Senior Leadership Team. An "Investigating Officer" will be appointed to take charge of the investigation on a day to day basis, this will normally be the Vice Principal (Finance & Resources).

5.3.3. The Investigating Officer will appoint an investigating team, this could comprise staff from outside the College.

5.3.4. Where initial investigations reveal that there are reasonable grounds for suspicion, and to facilitate ongoing investigation, it may be appropriate to

suspend an employee against whom an accusation has been made. This decision will be taken by the Principal, in consultation with the HR Manager and the Investigating Officer. Suspension should not be regarded as disciplinary action nor should it imply guilt. The suspended member of staff may appeal to the Principal if not satisfied with the conduct of the Investigating Officer in line with the College Appeals Procedure.

5.3.5. It is important from the outset, to ensure that evidence is not contaminated, lost or destroyed. The investigating team will therefore take immediate action to secure physical assets, including computers and any records thereon, and all potentially evidential documents. They will also ensure, in consultation with management, that appropriate controls are introduced to prevent further loss.

5.3.6. The Investigating Officer will ensure that a detailed record of the investigation is maintained. This should include a chronological file recording all details of telephone conversations, discussions, meetings and interviews (with whom, who else was present and what was said), details of documents reviewed, tests and analysis undertaken, the results and their significance. Everything should be recorded, irrespective of the apparent significance at the time.

5.3.7. All interviews will be conducted in a fair and proper manner. Where there is a possibility of subsequent criminal action, the police will be consulted and interviews may be conducted under caution in compliance with the Police and Criminal Evidence Act (PACE) which governs the admissibility of evidence in criminal proceedings.

5.3.8. The findings will be reported to the Principal, who in consultation with the HR Manager and the Investigating Officer will determine what further (if any) action should be taken.

5.4. Liaison with Police and the College Auditors

5.4.1. The police generally welcome early notification of suspected fraud, particularly that of a serious or complex nature. The Principal and Investigating Officer will determine if and when to contact the police. The Investigating Officer will report suspected fraud to the College's internal auditors at an appropriate time.

5.4.2. All staff will co-operate fully with any police or internal audit enquiries, which may have to take precedence over any internal investigation or disciplinary process. However, wherever possible, teams will co-ordinate their enquiries to maximise the effective and efficient use of resources and information.

5.5. Initiation of Recovery Action

5.5.1. The College will take appropriate steps, including legal action if necessary, to recover any losses arising from fraud, theft or misconduct. This may include action against third parties involved in the fraud or whose negligent actions contributed to the fraud.

5.6. Reporting Process

5.6.1. Throughout any investigation, the Investigating Officer will keep the Principal informed of progress and any developments. If the investigation is long or complex, interim reports will be made to the Audit Committee. These reports will be in writing.

5.6.2. On completion of the investigation, the Investigating Officer will prepare a full written report, for the Chair of Audit Committee and Principal, setting out:

- Background as to how the investigation arose
- What action was taken in response to the allegations
- The conduct of the investigation
- The facts that came to light and the evidence in support
- Action taken against any party where the allegations were proved
- Action taken to recover any losses, including any insurance claims
- Recommendations and/or action taken by management to reduce further exposure and minimise any recurrence.

5.6.3. A copy of the report will be submitted to the Audit Committee.

5.6.4. In order to provide a deterrent to other staff a brief anonymised summary of the circumstances will be published on the College Intranet.

5.7. Communication with Funding Bodies

5.7.1. Irrespective of the amount involved, the College must inform the Funding Bodies of any fraud or irregularities pertinent to the use of the funding grant and with regard to the financial memorandum. This would normally be done at the same time as internal auditors were informed.

Dos & Don’ts

DO	DON’T
Make a note of your concerns	**Be afraid of your concerns**
Record all relevant details, such as the nature of your concern, the names of parties you believe to be involved, details of any telephone or other conversations with names, dates and times and any witnesses. Notes do not need to be overly formal, but should be timed, signed and dated. Timeliness is most important. The longer you delay in writing up, the greater the chances of recollections becoming distorted and the case being weakened.	The Public Interest Disclosure Act provides protection for employees who raise reasonably held concerns through the appropriate channels. You will not suffer discrimination as a result of following these procedures and the matter will be treated sensitively and confidentially.
Retain any evidence you have	**Convey your concerns to anyone other than authorised persons**
The quality of evidence is crucial and the more direct and tangible the evidence, the better the chances of an effective investigation.	There may be a perfectly reasonable explanation for the events that give rise to your suspicion. Spreading unsubstantiated concerns may harm innocent persons.
Report your suspicions promptly	**Approach the person you suspect or try to investigate the matter yourself**
In the first instance, report your suspicions to your line manager. If this action is inappropriate further guidance on disclosure can be found in the fraud response plan.	There are special rules relating to the gathering of evidence for use in criminal cases. Any attempt to gather evidence by persons who are unfamiliar with these rules may destroy the case.