VISION West Nottinghamshire College

Anti-Fraud, Bribery and Corruption Policy

Contents

Summary of policy

West Nottinghamshire College conducts itself in a legal and ethical manner and is committed to the prevention of fraud, bribery and corruption. The College recognises that under the Economic Crime and Corporate Transparency Act 2023, the organisation has a responsibility to minimise fraud and not to benefit from fraud.

The purpose of this policy is to provide definitions of fraud, bribery and corruption, and define authority levels, responsibilities for action and reporting lines in the event of suspected, attempted or actual fraud, bribery or irregularity.

Fraud

West Nottinghamshire College operates a zero-tolerance attitude to fraud and requires staff, students and our partners to act honestly and with integrity at all times and to report all reasonable suspicions of fraud.

Bribery

The Bribery Act 2010 requires staff and postgraduate research students to not, either directly or indirectly:

- Offer, give, solicit or accept any bribe, either in cash or any other form of reward, to or from any person or company, wherever they are located and whether they are a public official or body, or private person or company.
- Give or retain any commercial, contractual or regulatory advantage through unethical or illegal means when conducting business on behalf of West Nottinghamshire College or its subsidiaries.

Staff and postgraduate research students must understand and strictly comply with the UK anti- bribery laws in all countries of the world.

Corruption

Corruption is the misuse of power for personal gain. Staff and students must act with integrity at all times and must ensure their activities, interests and behaviours do not conflict with this obligation, regardless of their seniority.

Reporting suspected incidents of fraud, bribery and corruption

Staff should report all suspected or actual incidents of fraud, bribery or other irregularity without delay to the Finance Director.

Where staff and students feel unable to report in this way, they should report this through.

West Nottinghamshire College's Whistleblowing Policy.

Scope

This policy applies to West Nottinghamshire College employees, students, other members of West Nottinghamshire College, and any other associated person acting on West Nottinghamshire College's behalf.

An associated person is someone who provides services to West Nottinghamshire College or acts on West Nottinghamshire College's behalf, and could be an employee of any type, consultant, agent, and/or other form of intermediary and subsidiary.

For the purposes of fraud, this policy applies to all students contracted with West Nottinghamshire College, no matter where they are situated, including students studying with collaborative provision and apprentices.

References to "staff and students" within this document cover all these categories of individuals.

Related Documentation

Refer to the following documentation in conjunction with this document:

Internal guidance

All

- Whistleblowing Policy
- Financial Regulations

External guidance

- Bribery Act Guidance and Economic Crime and Corporate Transparency Act 2023 (published by Ministry of Justice)
- Corporate Code of Ethics (published by Chartered Institute of Purchasing and Supply)
- Professional Body Code of Ethics (for staff who are members of professional bodies)
- DFE Fraud awareness good practice guide https://www.gov.uk/government/publications/fraud-awareness-good-practice-for-education-and-training-providers/fraud-awareness-good-practice-for-education-and-training-providers#preventing-fraud

---

Introduction

West Nottinghamshire College conducts its business in a legal and ethical manner, and operates a zero-tolerance attitude to fraud, bribery and corruption.

Staff and students are responsible for acting honestly and with integrity, and they must ensure that their activities, interests and behaviours do not conflict with these obligations, regardless of their seniority. Staff and students must report all reasonable suspicions of fraud and bribery.

Policy

1. Purpose

1.1 The purpose of this policy is to provide definitions of fraud, bribery and corruption, and to define authority levels, responsibilities for action and reporting lines in the event of suspected, attempted or actual fraud, bribery orirregularity.

---

2. Policy principles and strategy to counter fraud

2.1 West Nottinghamshire College has a zero-tolerance approach to fraud, bribery and corruption; as such, all forms of fraud, bribery and corruption are prohibited.

2.2 This policy applies to West Nottinghamshire College officers, employees, other members of West Nottinghamshire College, and any other associated person acting on West Nottinghamshire College's behalf. It applies to all of West Nottinghamshire College's activities and operations and to all of its dealings and negotiations with third parties in all countries in which its employees, agents, partners and associates operate.

2.3 **Counter fraud strategy and risk assessment**

- West Nottinghamshire College will address risks of fraud, bribery and corruption by ensuring that adequate and proportionate measures are developed and implemented to mitigate them. Annually a **fraud risk assessment** will be presented to the Audit Committee. The actions from this assessment will be reviewed at each Audit committee meeting.

- Financial regulations and procedures will seek to ensure clear segregation of duties and appropriate spend levels.

- Lessons learnt will be used to revise job roles and processes to ensure strong and appropriate controls are in place.

- the DFE Fraud awareness: good practice guide will be reviewed annually and used to identify cross sector areas of risk that should be considered by the college.
- The Audit Committee will ensure that an appropriate Internal Audit programme remains in place, which addresses the key organisational risk and ensures external oversight of internal controls.
- The College will link with other sector organisations to share intelligence about key risks and gain information about lessons learnt.
- The college will prioritise cyber security to seek to ensure that external attempts to subvert college systems to secure resources are minimised.
- High risk areas will be monitored via the College's risk register.
- Policies and Procedures will be amended in the light of any lessons learnt.

---

3. Definition of fraud

3.1 Fraud personas

- Fraud personas (initially developed by the Commonwealth Fraud Prevention Centre) are linked to the way somebody is contributing to a fraud and help us understand the kind of behaviours that a fraudster might display. Personas include:
- a corruptor – who abuses their position of entrusted power.
- a deceiver – who makes others believe something to be true which isn't.
- an enabler – who allows a fraud they know about to happen.
- an exploiter – who uses information they are aware of to make dishonest gain.
- a fabricator – who invents or produces false documents and information.
- an impersonator – who pretends to be somebody else to make personal gain.
- an organised group – who work in a co-ordinated way to make dishonest gain.

3.2 Fraud describes a number of activities including theft, false accounting, embezzlement, bribery and deception. The Fraud Act 2006 defines three classes of fraud:

- False representation: a person commits fraud by intentionally and dishonestly making a false representation. A false representation includes intentionally giving a misleading or untrue statement.

- Failing to disclose information: a person commits a fraud if they dishonestly fail to disclose information.
- Abuse of position: a person commits a fraud if they dishonestly abuse their position.

3.3 To have committed a fraud, a person must have acted dishonestly and with the intent to:

- make a gain for themselves or anyone else; and/or
- cause loss to anyone else; or expose anyone else to a risk of loss.

4. Definition of corruption

4.1 Corruption is the misuse of power for personal gain.

5. Definition of bribery

5.1 Bribery is where a financial or other advantage is offered as a reward to another party to persuade them to carry out their functions improperly. Bribery can be through the offering, promising, giving, demanding or accepting of an advantage such as gifts, hospitality, fees, rewards, jobs, internships, examination grades or favours.

5.2 An action is still classed as bribery regardless of whether the bribe is given or received directly or through a third party or whether it is for the benefit of the recipient or someone else.

5.3 Staff and students are required by the Bribery Act 2010 to not either directly or indirectly:

- Offer, give, solicit or accept any bribe, either in cash or any other form, to or from any person, company or other party. This applies no matter where that person is located and whether they are a public official or body, or a private person or company.
- Give or retain any commercial, contractual or regulatory advantage through unethical or illegal means when conducting business on behalf of West Nottinghamshire College or its subsidiaries.

5.4 Staff must understand and strictly comply with the UK anti-bribery laws in all countries of the world. There is further guidance available on facilitation payments, which are common in some countries, and this is also outlawed under the Bribery Act.

5.5 The action or exchange of a bribe does not need to have taken place – promising to give or agreeing to receive a bribe would be considered bribery.

5.6 Arrangements with third parties will be subject to clear contractual terms, including specific provisions requiring them to comply with standards and procedures relating to the prevention of bribery and corruption. West Nottinghamshire College will not engage, or continue business with, any individual or third party who we know or reasonably suspect of engaging in fraud, bribery or corruption.

5.7 Staff will not suffer penalty or other adverse consequences for refusing to pay a bribe, even if a refusal may result in loss of business.

---

6. Types of Fraud

6.1 Fraud is nothing new but over time it has become increasingly sophisticated as technology has improved. The development of artificial intelligence (AI) will bring further risks. Fraudsters use a whole range of methods to trick their victims and evolve their tactics over time. They can also pressure their targeted victims into making quick decisions, potentially overriding controls in place. Vigilance is important to prevention. Even something claiming to support fraud prevention might actually be a fraud itself. Some of the most commonly used methods in the education sector include the following.

6.2 Cyber fraud

6.3 This has increased rapidly as the internet has expanded. Cyber fraud is a term used to describe any kind of online fraud, but the most common forms are listed here.

6.4 Phishing (electronic impersonation)

- Emails or other messages claiming to be from reputable sources are sent to individuals and organisations trying to get the recipient to reveal personal information such as passwords and credit or debit card information.
- The information is then used to defraud the person who has supplied it or is sold on to other potential fraudsters. Fraudulent use of electronic signatures is a growing problem and emphasises the importance of using secondary identity checks and software to prevent documents being amended.
- Similar practices using different methods of communication include:
- smishing - specific to the use of messages via mobile phone.
- vishing - phone calls and voicemail messages from fraudsters.
- quishing - fake QR codes.
- As an example, a phishing attack might aim to get sensitive passwords used by providers which would give the fraudster access to a provider’s bank account. The attack may involve impersonation of the leaders of educational institutions to make a request appear genuine.

6.5 Malware

- Malware is a collective term for a range of online threats including:

- Viruses.
- Spyware.
- Adware.
- Ransomware.
- It is malicious software which can cause harm to or impede the use of a computer, server, or network infrastructure with or without the knowledge of the user. This could lead to user harm.
- Cybercriminals typically use malware to access and extract data, which they use to make financial gain from their victims.
- An example of malware is ransomware. This involves cybercriminals blocking organisations from accessing their own files and a ransom is then demanded to regain access to the files. This is a risk for the education sector, which holds lots of sensitive information, including data relating to children. It can also prevent providers from being able to operate effectively, if, for example, it is impossible to access files such as lesson plans.
- A malware attack can happen if a user:
- Opens a malicious attachment or link, assuming it is legitimate.
- Visits an infected website, leading to malware being downloaded and installed without the user's knowledge – once on the system, if the malware is not identified and dealt with swiftly, it can easily spread without user interaction and infect multiple networks.
- Cybercriminals sometimes target organisations when they are at their most vulnerable. Providers should:
- Be especially vigilant during holiday periods when they might have limited staffing.
- Make sure they are aware of any minimum cyber standards they need to meet in their sector in order to qualify for funding or be eligible for insurance should they be the victim of a cyber-attack.

6.6 Artificial intelligence (AI)

- AI can be of real benefit when used appropriately and effectively but is also a new tool fraudsters can use to deceive.
- AI enables fraudsters to impersonate others by creating deep fake videos and clone voices. This can convince victims that the person or situation they are dealing with is genuine. AI also makes it easier to combine real and fake data and to create realistic forged documents that can be used to verify identity or provide certification.
- In the education sector AI is a real threat with regard to the:
- Use of copied or impersonated voices and imagery with the aim of extorting money and causing reputational damage – impersonating educational leaders such as CEOs, principals and trustees is a significant fraud risk in the education sector according to research from Lloyds and TSB bank.
- Authenticity of work submitted by students.
- Creation of certificates evidencing qualifications.
- Creation of content potentially harmful to young people.
- The Public Sector Fraud Authority's Introduction to AI with a focus on counter fraud has more information.

6.7 Invoice fraud

- This is also known as mandate fraud. Fraudsters pose as genuine suppliers and usually advise of a change in payment details. They may ask for payment, urgently putting pressure on the target of the fraud.

- The education sector is vulnerable to fraud due to the number of suppliers required across the country to make the system work. Providers should:
- Always double check with suppliers before making a payment to a newly provided bank account.
- Use contact details they have reliably used previously and not contact details provided in the communication advising of the change of payment detail.

6.8 Certificate fraud or qualification fraud

- This is a big issue for providers and awarding bodies. Anyone who falsely creates a qualification certificate or alters a genuine one and presents it as real is committing fraud.
- The main risks for providers are:
- They enrol a learner based on a fake certificate or qualification and may claim funding that the learner is not eligible for.
- They employ an individual based on a fake certificate or qualification, who is unsuitable for the role and could be a safeguarding risk.
- Individuals claim to have studied and achieved a qualification with the provider which is not a genuine qualification – this is potentially damaging to the reputation of the provider and can affect confidence in the integrity of the courses and qualifications they offer.
- Falsified assessment of student work where unwarranted achievement might be recorded or claimed for financial or other benefit to a provider or assessor.
- Certificate or qualification fraud can also be a breach of copyright and intellectual property rights, where genuine or fake logos of organisations are included on the certificate.

6.9 Banking fraud

- An attempt by fraudsters to get people to send money to bank accounts they have set up.
- The most common examples of this in the education sector are emails sent to providers, which falsely claim to be from suppliers, a provider has used and give bank account details for payment to be sent to.
- Providers should:
- Be aware of fake online banking websites when using search engines to find their bank.
- Be aware of phone calls pretending to be from banks, where people are directed to fake online banking – fraudsters can have the capability to influence the call display, so it genuinely appears to be the bank which is calling.
- Never give out payment details over the phone to somebody who has called them.

6.10 Money laundering

- This is where the proceeds from criminal activity are used for, or transferred to, a legal source of funding to conceal the money's origin. In the education sector, providers should be wary of receiving large amounts of upfront fees or unexpected donations without a rational explanation. Students and young people are often targeted to be used as 'money mules' where fraudsters launder money through somebody's bank account to make it harder to track.

6.11 Procurement fraud

- Providers should be vigilant against various types of procurement fraud. Examples include:
- Fake invoices containing incorrect bank details or sending duplicate invoices for the same work.
- Suppliers putting in genuine bids for work that an education provider has put out to tender, but the suppliers are working together to inflate the price beyond the true market cost – using a procurement framework with guidelines and processes for handling a procurement can mitigate against the risk of procurement fraud.
- The fraud methods listed above are not exhaustive and providers should be wary of any unusual activity, particularly requests for payments which fall outside of their normal established processes. A regular cross-check of supplier bank details can assist with this.

6.12 Internal fraud v External fraud

- Internal fraud is when an employee or employees commit (or attempt to commit) a fraud against the organisation they work for. These can be hard to detect, as employees have inside knowledge of systems and processes the organisation uses and are aware of system weaknesses and vulnerabilities.
- Internal fraud can include:
- Falsified travel expenses.
- Theft of assets.
- Accepting inappropriate gifts and hospitality.
- Plots to transfer money out of the organisation.
- Internal frauds sometimes occur as a result of collusion from unknown and undeclared interests and relationships. Providers need to have processes in place to help them prevent and detect internal fraud, including being aware of any conflicts of interest.
- External fraud is where parties outside of an organisation target an organisation illegally for some kind of financial benefit.

7. Key responsibilities

7.1 The Director of Finance/CFO is responsible for developing, implementing and maintaining adequate systems of internal control to prevent and detect fraud, bribery and corruption.

7.2 Senior managers are responsible for familiarising themselves with the types of fraud, dishonesty, bribery and corruption that might occur in their directorates or departments, monitoring compliance with internal controls and agreed policies and procedures and notifying their line manager (or any of the people specified in the procedure below) or any indications of fraudulent activity.

7.3 All staff are responsible for protecting the college’s interests and not engaging in activity which could be interpreted as fraud, dishonesty, bribery or corruption. If staff become aware of activity which might be fraud, dishonesty, bribery or corruption, they must report this to their line manager or senior manager. If a member of staff feels unable to do this, they should consult the Whistleblowing Policy for further guidance.

7.4 Students must act with integrity in respect of their studies, and provide full, accurate and truthful information when seeking any form of support, financial assistance and integrity of work submitted for the award of qualifications. They should report any activity of the employees of West Nottinghamshire College, or other staff which they consider may be in breach of this policy.

8. Communication

8.1 West Nottinghamshire College ensures that its fraud, bribery and corruption prevention, and associated policies and procedures, are embedded and understood throughout the organisation through internal and external communication, including training that is proportionate to the risk itfaces.

8.2 The Executive are responsible for ensuring the communication of West Nottinghamshire College's Anti-Fraud, Bribery & Corruption Policy and other relevant policies to associated person(s). The Executive will monitor and review their procedures and action plans to ensure their suitability, adequacy and effectiveness in relation to this policy and implement improvements as appropriate.

8.3 Staff who process orders or arrange purchasing transactions will receive the policy and training to support them to identify suspect activity and clarify expectations of them.

9. Due diligence

9.1 West Nottinghamshire College will apply due diligence procedures, taking a proportionate and risk-based approach, in respect of persons and organisations that perform, or will perform, services for or on behalf of West Nottinghamshire College, in order to mitigate identified bribery risks.

9.2 Where appropriate, senior managers will complete sufficient due diligence when entering into arrangements with others, to ensure they are not acting corruptly, and will periodically monitor their performance to ensure ongoing compliance. They will take appropriate action in response to any information uncovered as a result of due diligence which gives rise to concern and report any such actions to the Finance Director.

Procedure

10. Implementation and enforcement of procedure

Preventing Fraud

10.1 It is unrealistic to think fraud can be stopped completely, but measures to prevent and minimise fraud with the College has put in place are to:

10.2 Review Fraud Risk annually and create an action plan.

10.3 Give specific fraud awareness responsibilities to named job roles with the Risk Assessment and Action Plan.

10.4 Have a clear policy or response plan including robust internal systems to counter-fraud, including how specific fraud risks are identified, assessed and managed.

10.5 Ensure that staff at all levels have good awareness of fraud threats, including relevant regular training on emerging and new technology-based frauds to help create a counter fraud culture where challenge and reporting are encouraged.

10.6 Ensure that any sub-contractors also manage fraud risks and are not a fraud threat themselves.

10.7 Educate students and learners on fraud threats.

Key Risk areas and the lead responsible person

10.8 The table below shows key roles.

Key Fraud Actions and Responsibility

Risk Area	Responsible Individual
Maintaining the Counter Fraud Policy	Director of Finance/CFO
Undertaking Fraud Risk Assessment	Director of Finance/CFO
Reporting Fraud to Agencies	Director of Finance/CFO
Ensuring training to support a fraud awareness culture	Director of Finance/CFO
Development of Internal Controls to limit the opportunity for Fraud	Director of Finance/CFO
Due Diligence for Staff and Appointments	Director of HR
Due Diligence of IT suppliers	Director of Estates/IT
Due Diligence of Estates Contractors	Director of Estates/IT
Due Diligence of Education Subcontractors	Vice Principal Curriculum
Due Diligence of Other suppliers	Director of Finance/CFO
Internal control process to limit cybercrime	Director of Estates/IT
Development of internal controls to grant and remove access to IT systems	Director of Estates/IT
Financial Controls to prevent unauthorised payments	Director of Finance/CFO

Internal controls to minimise risk on claims for pay and expenses	Director of HR
Development of Internal Controls to limit malpractice by staff and students relating to qualifications	Vice Principal Curriculum
Security of assets	Director of Finance/CFO
Security of Sites	Director of Estates/IT

Reporting fraud, bribery and corruption

10.9 Staff should report without delay all other suspected or actual incidents of fraud, bribery or corruption allegedly perpetrated to the Finance Director.

- Where staff and students feel unable to report in this way, they should report this through West Nottinghamshire College's Whistleblowing Policy. This policy provides guidance on alternative reporting. Staff and external parties can report to alternative roles, including the Principal or the Chair of the Audit Committee.

Referral to external agencies

10.10 The Chair of the Audit Committee will decide at what stage a case should be reported to the police or other external agency such as the Serious Fraud Office (SFO). Certain offices carry criminal liability for individuals concerned, and sanctions include significant fines and/or imprisonment.

10.11 West Nottinghamshire College must inform the DFE about actual or suspected cases of fraud as required by the College Financial Handbook. The Director of Finance/CFO is responsible for informing the DFE or any such incidents. Liaison with other external bodies (for example, the Student Loans Company) will be undertaken as appropriate to individual cases.

10.12 By informing the DFE, West Nottinghamshire College will be fulfilling its duty to report serious incidents arising from fraud and theft to the CharityCommission.

Prevention of further loss

10.13 Where initial investigation provides reasonable grounds for suspicion of fraud or bribery, the Director of Finance/CFO will decide how to prevent further loss. If the individual under suspicion is an employee or student, this may require the suspension of the person(s) alleged to have committed the suspected fraud or irregularity. For an employee, this suspension could be with or without pay. It may be necessary to plan the timing of the suspension to prevent the individual(s) from destroying or removing evidence that may be needed to support disciplinary or criminal action.

10.14 The Director of Finance/CFO will, as necessary, consult with the IT, Estates and Learning Resources Director about preventing subsequent access to West Nottinghamshire College property, and may authorise the withdrawal of permissions for West Nottinghamshire College computer systems.

10.15 The Director of Finance/CFO will consider whether it is necessary to investigate systems other than that which has given rise to suspicion, through which the individual(s) may have had opportunities to misappropriate West Nottinghamshire College's assets.

Establishing and securing evidence

10.16 Put a fraud action plan in place for each reported incident.

10.17 The Director of Finance/CFO will:

- Maintain familiarity with West Nottinghamshire College's disciplinary procedures, to ensure that evidential requirements are met during a fraud investigation.
- Ensure that staff and students involved in fraud investigations are familiar with and follow rules on the admissibility and other evidence of criminal proceedings. This will usually involve the appointment of specialist fraud investigators; and
- Ensure that the internal audit team are able to provide advice in accordance with West Nottinghamshire College's Whistleblowing Policy.

Recovery of losses

10.18 Recovering losses is a major objective of any fraud and/or bribery investigation. The Director of Finance/CFO will ensure that, in all investigations, the amount of any loss will be quantified. Repayment of losses should be sought in all cases.

10.19 The Director of Finance/CFO will, as necessary, consider seeking legal advice, on the recovery of losses and costs through the civil courts.

References for employees disciplined or prosecuted for fraud

10.20 Any request for a reference for a member of staff who has been disciplined or prosecuted for fraud shall be referred to HR. HR will consider employment law when preparing any answer to a request for a reference.

Reporting to governors

10.21 Any incident matching the criteria in the DFE's College Financial Handbook shall be reported without delay by the Director of Finance/CFO to the Audit Committee.

10.22 Any variation from the approved Anti-Fraud, Bribery and Corruption Policy, together with reasons for the variation, will be reported promptly to the Audit Committee.

10.23 The Audit Committee will be kept informed of the progress of any investigations relating to impropriety including:

- 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; and
- Any action needed to strengthen future responses to fraud, with a follow-up report on whether the actions have been taken.

10.24 This report will normally be presented as part of the regular updates provided by the Finance Director.

11. Non-compliance

11.1 West Nottinghamshire College will investigate all instances of actual, attempted and suspected fraud, bribery and corruption committed by staff, students, consultants, suppliers and other third parties and will seek to recover funds and assets lost through fraud. Where individuals do not comply with this policy, they risk suspension or loss of employment and may be reported to external agencies such as the police.

12. Methods of appeal

12.1 Disciplinary procedures for staff and students contain information on the right of appeal. If a fraud or bribery is reported to external agencies – for example, the police – the subject will have a right of appeal in the context of any action the agency might choose to take.

Glossary of terms

Bribery

See definition under section 5 of this policy.

Corruption

See definition under section 4 of this policy.

Deception

The act of hiding the truth, usually to gain an advantage.

Embezzlement

To secretly take money that is in your care or that belongs to an organisation or business that you work for.

Facilitation Payment

A facilitation payment is a payment which is made with the intention of securing or speeding up an administrative process. A common example is a government official being given money or goods to perform an existing duty.

Fraud

See definition under section 3 of this policy.

Intermediaries

An organisation that makes business or financial arrangements between companies or organisations that do not deal with each other directly.

Subsidiaries

Companies which are owned by the college or in the case of external companies by larger companies.

False accounting

This involves an employee or organisation altering, destroying or defacing any account, or presenting accounts from an individual or organisation that does not reflect their true value or the financial activities of the organisation.

Further clarification

Staff can contact the Director of Finance/CFO via email: finance@wnc.ac.uk