University of Staffordshire

Fraud Prevention

Including policies

Contents

Introduction

What is Fraud?

Fraud is any act of deception intended for personal gain or to cause a loss to another party. This includes both financial and non-financial gain and loss.

For the University this means:

Misappropriation or theft of cash, stock, or other assets
This might include the theft of stationery for private use, or the unauthorised use of University vehicles, computers or other equipment.

Purchasing fraud
This can include approving or paying for goods not received, paying inflated prices for goods and services, or accepting any bribe.

Misstating claims or eligibility for other benefits
Such as overstating or making false travel and subsistence claims.

Accepting pay for time not worked
This can include failing to work full contracted hours, making false overtime claims, or falsifying sickness.

Record fraud, often via computers
Such as altering or substituting records, duplicating or creating spurious records, or destroying or suppressing them.

Intellectual Property (IP) theft
Such as claiming university intellectual property as your own, or otherwise using or selling university IP for your own personal gain. Staff should not benefit financially from the University's name unless agreement is reached under the University's IPR and Commercialisation policy.

How big a problem is it?

Fraud is, by its nature, hidden, which means it's hard to know exactly how big a problem it is.

Unfortunately, financial loss is only part of the picture. Fraud also poses a reputational risk to large organisations such as Universities. In today's 24–hour news cycle, Universities that publicly suffer frauds can face a significant impact to their standing in the community and with other stakeholders. Even when frauds don't become public knowledge, the subsequent investigations and actions can drain staff time and energy, and negatively impact staff morale. All this has a hidden cost.

Who does it involve?

Relatively few frauds are committed by professional fraudsters or organised criminals, and many aren't even premeditated. The uncomfortable reality is that most people have the capacity to commit fraud under the right circumstances. The likelihood that someone, such as a member of staff, will commit fraud could depend on some of the following things:

Motivation
This is the financial or emotional pressure or incentive to commit fraud. It might stem from the sudden need to increase income, such as if a partner loses their job. It might be the desire to purchase something expensive, or a financial need to meet an addiction. It may even be driven by an abusive relationship or blackmail.

Opportunity
This is the capacity and opportunity to commit fraud without getting caught. People in positions of relative power, where there are insufficient checks and oversight, can have many opportunities to commit fraud. Opportunities can also arise just from poor management or insufficient management processes.

Rationalisation
This is the ability of fraudsters to excuse or justify their actions. The likelihood of someone committing fraud depends on if they can justify it to themselves. They might tell themselves that no one will be a victim or get hurt. They might say that they need the money more than the organisation does. They might say that it's only a small amount, so it doesn't really matter.

What can you do about it?

You have two options. You can stick your head in the sand and pretend that the University doesn't have a fraud problem, and hope that no frauds get exposed on your watch. In our current day and age, this is a risky strategy.

The second option is to start now in implementing an effective counter-fraud programme that prevents potential fraud, identifies and minimises frauds that do occur, and actively manages the post-fraud situation to mitigate reputational risk and maintain morale.

This involves a range of activities and approaches, many of which are mentioned or covered in the rest of this handbook.

These include:

- Assessing the risk of fraud in the University
- Raising awareness of fraud across the University
- Putting in place appropriate policies and procedures
- Implementing effective internal controls in areas of risk
- Enabling safe fraud-reporting and effective internal communication

At University of Staffordshire, we manage our risks using the Risk Management Framework (a Managing Risk Handbook is available separately) as fraud, bribery and corruption are a significant risk to the University, it is important that the correct policy's and procedures are in place to ensure we manage this risk.

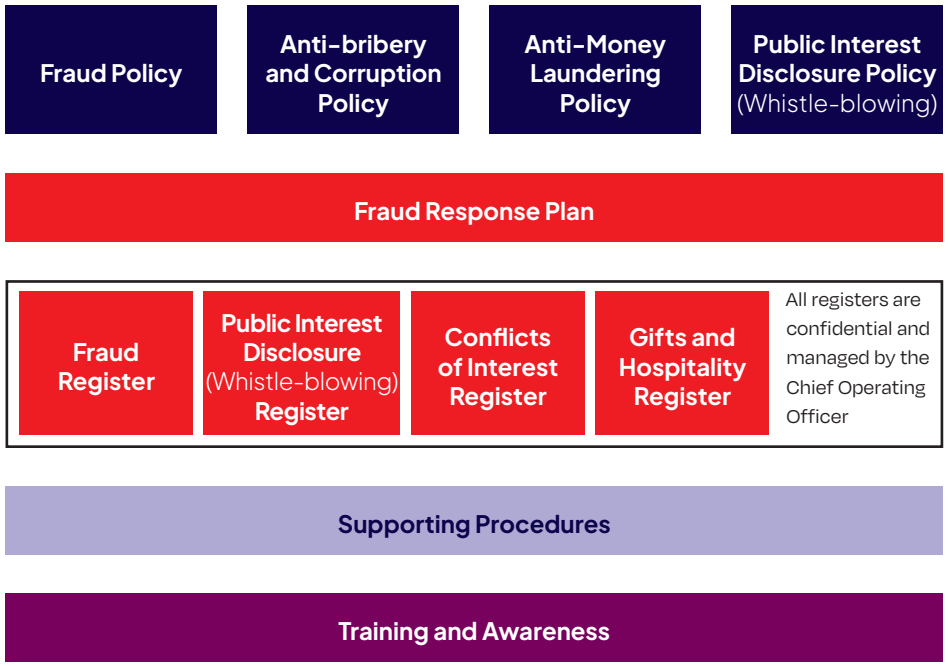
This handbook is made up of:

- **Fraud Response Plan**
  This document provides guidance on how a suspected fraud should be reported and how this is dealt with by relevant parties within the University.
- **Counter Fraud Policy**
  Provides guidance on how to identify and report suspected fraud.
- **Anti-bribery and Corruption Policy**
  Provides guidance on how to identify and report suspected bribery and corruption.
- **Anti-money Laundering Policy**
  Provides guidance on how to identify and report suspected money laundering.
- **Public Interest Disclosure Policy** (whistle-blowing)
  To assist individuals who believe they have discovered malpractice or impropriety and how to report any suspicions.

It is important as an employee of the University that you are aware of the policies and procedures and report any suspicions as indicated in these documents or contact the Head of Risk and Resilience if you have any queries or questions.

As part of the reporting and recording of any suspicions registers are maintained by the Head of Risk and Resilience. The registers are private and confidential and all suspicions raised are treated with the upmost confidentiality.

Fraud Framework



Fraud Response - Initial Steps

1.0 Purpose

In summary, the purpose of the Fraud Response Plan is to define authority levels, responsibilities for action and reporting lines in the event of a suspected fraud or financial irregularity. The use of the plan should allow the University to:

- Respond quickly and professionally to any suspicion or suggestion of fraud or irregularity
- Assign responsibility for initial and subsequent investigation
- Prevent further loss
- Establish and secure evidence necessary for disciplinary and/or criminal action against those who have committed the fraud
- Notify Office for Students (OfS) if required
- Notify the University's insurers if required
- Minimise and recover losses
- Establish an internal and external communications strategy and process
- Establish the need (or otherwise) for external specialist involvement
- Establish the need for police notification, and the lines of communication
- Review the circumstances of the fraud, actions taken to prevent a recurrence and any action needed to strengthen future responses to fraud
- Deal with HR-type issues such as references in relation to staff disciplined and/or prosecuted for fraud

2.0 Guidance when receiving a report of fraud

Listen to the concerns of your staff and treat every report you receive seriously and sensitively. Make sure that all staff concerned are given the opportunity to raise their concerns, bearing in mind that they could be distressed, upset and/or frightened.

- Reassure your staff that they will not suffer because they have told you of their suspicions, as long as they are made in good faith
- Get as much information as possible. Do not interfere with any evidence and make sure it is kept in a safe place
- Ask the member of staff to keep the matter fully confidential in order that it can be investigated without alerting the suspected/alleged perpetrator.

3.0 Fraud response key stages

This Handbook covers Stages 1&2 Stages 3–12 are available on request from the Head of risk and Resilience

1 Initial response
2 Initial reporting
3 Meeting of the Fraud Response Team
4 Lead investigation plan
5 Role and responsibility of the lead investigator
6 Establishing and securing evidence
7 Prevention of further losses
8 Interviews/statements
9 Police involvement
10 Recovering losses
11 Reporting (Fraud Register) Including notifying OfS
12 Investigation outcomes

Fraud – Initial response - Stage 1

A fraud or financial irregularity may be discovered in a variety of ways, from your own or a colleague's observations, someone from inside or outside the University 'blowing the whistle', financial controls identifying a discrepancy, internal or external audit discovering a problem or external bodies identifying an issue.

Irrespective of how a potential fraud is discovered, the following should always be borne in mind -

- Things to do
- Things not to do
- Things to remember

Things to do:

- Stay calm – remember you are a witness not a complainant
- If possible, write down your concerns immediately - make a note of all relevant details such as what was said in phone or other conversations, the date, the time and the names of anyone involved
- Consider the possible risks and outcomes of any immediate action you may take
- Make sure that your suspicions are supported by facts, as far as is possible at this stage.

Things not to do:

- Don't become a private detective and personally conduct an investigation or interviews
- Don't approach the person/persons potentially involved (this may lead to conflict, violence, him/her destroying evidence etc.)
- Don't discuss your suspicions or case facts with anyone other than those persons referred to below
- Don't use the process to pursue a personal grievance

Things to remember:

- You may be mistaken or there may be an innocent or good explanation - but this will come out in the investigation
- The fraud response and investigation process may be complex and relatively lengthy and, as a consequence, you may not be thanked immediately. Moreover, the situation may lead to a period of disquiet or distrust in the University despite you having acted in good faith

A fraud or financial irregularity may also come to light through:

- The University's Public Interest Disclosure Policy
- The University's disciplinary procedures
- The University's procedures for addressing research misconduct
- Disclosure by the person, or persons, involved.

Fraud – Initial reporting - Stage 2

All actual or suspected incidents should be reported immediately either:

- To the Chief Finance Officer, the Chief Operating Officer or the Head of Risk and Resilience
- Via the University's Public Interest Disclosure Policy (whistle-blowing) available on WorkVivo

If the disclosure directly involves or implicates any of the individuals identified above then the disclosure should be made to the Vice Chancellor and/or the Chair of Audit and Risk Committee as appropriate.

Fraud Motives

Fraud motives

Here is a list of generic fraud risks in HEI's this list provides generic indicators of potential fraud. These include personal and organisational motives for fraud, possible weakness of internal controls, transactional indicators and possible methods of committing and concealing fraud.

Possible Personal Motives

1. Personnel believe they receive inadequate compensation and/or rewards (recognition, job security, vacations, promotions etc.)
2. Expensive lifestyle (cars, trips etc.)
3. Personal problems (gambling, alcohol, drugs, debt, etc.)
4. Unusually high degree of competition/peer pressure
5. Related party transactions (business activities with personal friends, relatives or their companies)
6. Conflict of Interest
7. Disgruntled employee (recently demoted, reprimanded etc.)
8. Recent failure associated with specific individual
9. Personal animosity or professional jealousy

Organisational Motives

1. Organisation experiencing financial difficulty
2. Commercial are experiencing financial difficulty
3. Tight or under unusually tight time deadlines to achieve level of out puts
4. Organisational governance lacks clarity and direction
5. Organisations closely identified with/dominated by one individual
6. Organisation under pressure to show results (budgetary, exam results etc.)
7. Organisation recently suffered disappointment/reverses/consequences of bad decisions
8. Organisation wants to expand its scope, obtain additional funding
9. Funding award up for continuation
10. Organisation due for a site visit by auditors or other quality controllers
11. Organisation recently affected by new/changing conditions (regulatory, economic, environmental etc.)
12. Organisation faces pressure to use or loose funds to sustain future funding levels
13. Record of previous failure(s) by one or more organisational areas
14. Sudden change in organisation practice or pattern of behaviour

Internal Controls are Weak

1. Management demonstrates lack of attention to ethical values; lack of communication regarding importance of integrity and ethics, lack of concern about presence of temptations and inducements to commit fraud, lack of concern regarding instances of fraud, no clear fraud response plan or investigation policy
2. Management fails to specify needed levels of competence
3. Management displays a penchant for taking risks
4. Lack of an appropriate organisational and governance structure with defined lines of authority and reporting responsibilities
5. Institution lacks policies and communication relating to individual accountability and best practices e.g. procurement, travel and subsistence, use of alcohol, declarations of interest
6. Lack of personnel policies and recruitment practices
7. Institution lacks personnel performance appraisal measures or practices
8. Management displays lack of commitment towards the identification and management of risks relevant to the preparation of financial statements; does not consider significance of risks, likelihood of occurrence or how they should be managed
9. There is inadequate comparison of budgets with actual performance and costs, forecasts and prior performance, no regular reconciliation of control records and lack of proper reporting to governing body
10. Management of information systems is inadequate; no policy on information technology security, computer use and access, verification of data accuracy completeness or authorisation of transactions

11. There is insufficient physical security over facilities, assets, records, computers, data files, cash; failure to compare existing assets with related records at reasonable intervals
12. There is inadequate or inappropriate segregation of duties regarding initiation, authorisation and recording of transactions, maintaining custody of assets
13. Accounting systems are inadequate; ineffective method for identifying and recording transactions, no tracking of time periods during which transactions occur, insufficient description of transactions and to which account they should be allocated to, no easy way to know the status of funds on a timely basis, no adequate procedure to prevent duplicate payments or prevent missing payment dates, etc.
14. There is a lack of internal, ongoing monitoring of controls which are in place; failure to take any corrective actions, if needed
15. Purchasing systems/procedures inadequate; poor or incomplete documentation of purchase, payment, receipt; poor internal controls as to authorisation and segregation of duties
16. Subcontractor records/systems reflect inadequate internal controls
17. Management is unaware of or displays lack of concern regarding applicable laws and regulations e.g. Companies Acts, Charities Acts, Funding Agreement, Child Protection
18. Specific problems and/or reportable conditions identified by audits or other means of oversight have not been corrected. This may include a history of problems, a slow response to past findings or problems, or unresolved present findings
19. No mechanism exists to inform management and governors of possible fraud
20. General lack of management oversight

Transactional Indicators

1. Related party transactions with inadequate, inaccurate or incomplete documentation or internal controls (business/research activities with friends, family members or their companies)
2. Not-for-profit entity has a for-profit counterpart with linked infrastructure (shared board of governors or other shared functions and personnel)
3. Specific transactions that typically receive minimal oversight
4. Previous audits with findings of
    - questioned costs
    - evidence of non-compliance with applicable laws or regulations
    - weak internal controls
    - inadequate management response to any of above
    - a qualified opinion

5. Transactions and/or accounts which are difficult to audit or subject to management judgment and estimates
6. Multiple sources of funding with inadequate, incomplete or poor tracking, failure to segregate funds and/or existence of pooled funds
7. Unusual, complex or new transactions, particularly if occur at year end, or end of reporting period
8. Transactions and accounts operating under time constraints
9. Cost sharing, matching or leveraging arrangements where industry money or other donation has been put into a foundation (as in a foundation set up to receive gifts) without adequate controls to determine if money or equipment has been spent/used; whether it has gone to allowable costs and at appropriate and accurate valuations; outside entity such as foundation provided limited access to documentation
10. Travel accounts with
    - inadequate, inaccurate or incomplete documentation or poor internal controls such as appropriate authorisation and review
    - variances between budgeted amounts and actual costs
    - claims in excess of actual expenses
    - reimbursement for personal expenses
    - claims for non-existent travel
    - duplicate payments
11. Credit card accounts with inadequate, inaccurate or incomplete documentation or internal controls such as appropriate authorisation and review
12. Accounts in which activities, transactions or events involve handling of cash or wire transfers; presence of high cash deposits maintained with banks
13. Assets and inventory are of a nature to be easily converted to cash (small size, high marketability, lack of ownership identification, etc.) or easily converted to personal use (cars, houses, equestrian centres, villas etc.)
14. Accounts with large or frequent shifting of budgeted costs from one line item to another without adequate justification
15. Payroll (including fringe benefits) system with controls that are inadequate to prevent an individual being paid twice, or paid for non-delivery or non-existence; or outsourced but poor oversight of starters/leavers and payments
16. Consultant agreements which are vague as to work, time period covered, rate of pay, product expected; lack of proof that product or service actually delivered
17. Subcontract agreements which are vague as to the time period covered, the rate of pay, the product expected, or lack of proof that product or service actually delivered

Committing/Concealing Fraud

Possible methods of committing/concealing fraud

The following is a list of possible methods that you may recognise when someone is attempting to commit a fraud.

- Refusal or reluctance to turn over documents
- Unreasonable explanations
- Annoyance at questions
- Trying to control the audit process (timetables, access, scope)
- Individual blames a mistake on a lack of experience with financial requirements or regulations governing funding
- Promises of cooperation followed by subsequent excuses to limit or truncate co-operation
- Subtle resistance
- Answering a question that wasn't asked
- Offering more information than asked
- Providing wealth of information in some areas, little to none in others
- Explaining a problem by saying "we've always done it that way", or "someone at Xx told us to do it that way" or "Mr X said he'd take care of it"
- A tendency to avoid personal responsibility (overuse of "we" and "our" rather than "I"); blaming someone else
- Too much forgetfulness
- Trying to rush the audit process

Issues with documents such as:

- Missing documents
- Documents are copies, not originals
- Documents in pencil
- Altered documents
- False signatures/incorrect person signing
- Deviation from standard procedures (all files but one handled a particular way; all documents but one included in file, etc.)
- Excessive journal entries
- Transfers to or via any type of holding or suspension account
- Inter-fund loans to other linked organisations
- Records maintained are inadequate, not updated or reconciled
- Use of several different banks, or frequent bank changes; use of several different bank accounts
- Failure to disclose unusual accounting practices or transactions
- Uncharacteristic willingness to settle questioned costs
- Non-serial-numbered transactions or out-of-sequence invoices or other documents
- Duplicate invoices
- Eagerness to work unusual hours
- Access to/use of computers at unusual hours
- Reluctance to take leave
- Insistence on doing job alone
- Refusal of promotion or reluctance to change job
- Creation of fictitious accounts, transactions, employees, charges
- Writing large cheques to cash or repeatedly to a particular individual
- Excessive or large cash transactions
- Payroll cheques with unusual/questionable endorsements
- Payees have similar names/addresses
- Non-payroll cheques written to an employee
- Defining delivery needs in ways that can only be met by one source
- Continued reliance on person/entity despite poor performance
- Charging items to project account for personal purposes (books and supplies bought for family members, home gym equipment charged to project account etc.)
- Materials erroneously reported as purchased; repeated purchases of same items; identical items purchased in different quantities within a short time period; equipment not used as promised, doesn't work, doesn't exist.

5.0 Operative

This procedure was approved by the Audit and Risk Committee.

Fraud Prevention Policies

Counter Fraud Policy Cover

Policy Coversheet

Name of Policy:	Counter Fraud Policy
Purpose of Policy:	To define how the University manages fraud
Intended Audience(s):	All Staff
Approval for this Policy given by:	Audit and Risk Committee
Last Review Date:	February 2025
Review Due Date:	February 2026
Individual responsible for Review:	Head of Risk and Resilience
Authorising Department:	Corporate Services

Counter-fraud Policy

1.0 Policy Statement

1.1 The University is committed to the proper use of funds, both public and private. As a consequence, it is essential that everyone associated with the University - including staff, students, employees, contractors and third-parties are aware of the risk of fraud, corruption, theft and other activities involving dishonesty, in all its forms.

1.2 The University aims to reduce instances of fraud to the absolute practical minimum and to also put in place arrangements that hold any fraud to a minimum level on an ongoing basis. The University's approach to counter-fraud will be comprehensive, cost-effective and professional, using specialist expertise if, as and when required.

2.0 Definitions

2.1 Fraud can be defined as (i) wrongful or criminal deception intended to result in financial or personal gain and (ii) a person or thing intended to deceive others, typically by unjustifiably claiming or being credited with accomplishments or qualities. Both definitions are, clearly, directly applicable to the Higher Education sector.

3.0 Counter-Fraud Policy Objectives

3.1 Most organisations adopt a multi-faceted approach to fraud and the University is no exception. The eight key objectives of the University's Counter-Fraud Policy are:

- Establishment of a counter-fraud culture
- Maximum deterrence of fraud

- Active and successful prevention of any fraud that cannot be deterred
- Rapid detection of any fraud that cannot be prevented
- Professional investigation of any detected fraud
- Effective internal and external actions and sanctions against people found to be committing fraud, including legal action for criminal offences
- Effective communication and learning in relation to fraud, and
- Effective methods of seeking redress when/where fraud has been perpetrated

The overriding objective of the University's counter-fraud activity is to ensure that (i) fraud is seen as unacceptable by each and every stakeholder and (ii) counter-fraud is seen to have the unwavering focus of the University as a whole.

3.2 This document sets out the University's policy for dealing with suspected cases of fraud, including corruption, and includes summarised instructions about what to do, and who to contact/notify, should any fraud-related concerns arise.

3.3 At a practical level, fraud is deemed to be deliberate intent to deprive the University (and its associate activities) of money or goods through the falsification of any records or documents (e.g. submission of false invoices, inflated time records or travel claims and/or the use of purchase orders to obtain goods for personal use). This is an important distinction, intended to clarify the crucial difference between deliberate fraud and unintentional error, removing - wherever possible - any potential confusion or ambiguity.

4.0 Counter-fraud Policy

4.1 The University is absolutely committed to the highest standards of honesty, accountability, probity and openness in its governance. As a direct consequence of this, the University is committed (i) to reducing fraud associated with any of its activities, operations and locations to the absolute practical minimum and (ii) to the robust investigation of any fraud issues that should arise. Any such investigation will be conducted without regard to factors such as position, title or length of service.

4.2 In the case of an applicant who has not yet completed enrolment, Finance will contact the registry to withdraw the offer made to the applicant.

4.3 In the case of an enrolled student, Finance will speak to the student directly in order to establish the facts of the case, and if Finance believe

there is either a cause of welfare concern (the student has been misled by a third party into committing fraud) or an active attempt at fraud by the student, then these will be referred to student services/registry to be dealt with either as a welfare concern (with a follow up meeting with the student) or as a disciplinary matter through the normal regulatory route. Where any acts of fraud or corruption are proven, the University will make every endeavour to ensure that the perpetrator(s) are dealt with to the full extent of the law and University disciplinary policy/contractual processes (where a third-party is involved) and will also take every step to recover any and all losses in full.
It is the responsibility of everyone associated with the University - including staff, students, employees, contractors and third parties - to report any fairly based suspicions of fraud or corruption. The University has a "no retaliation" approach for people reporting reasonably-held suspicions, and concerns can be raised if necessary, under the University's Public Interest Disclosure Policy.

4.4 This policy applies to any fraud, or suspected fraud, involving everyone and anyone associated with the University - including staff, students, employees, contractors and third parties.

5.0 Common types of University and Higher Education Fraud

These can include, but are not limited to:

- Fraud involving cash, physical assets or confidential information
- Misuse of accounts
- Procurement fraud
- Payroll fraud
- Financial accounting fraud, including fees
- Fraudulent expense claims
- Reference, qualification and related employment fraud
- Recruitment and appointment fraud
- Bribery and corruption fraud
- Academic fraud including immigration, admissions, internships, examinations and awards
- Accommodation-related fraud, including preference and payment

6.0 Counter-Fraud Actions including Do's and Don'ts

6.1 Dos and Don'ts
Where there is suspicion that fraud or corruption has occurred, or is about to occur, then it is essential that the appropriate person within the University is contacted immediately; a list of appropriate persons and how to contact them is contained in Appendix 1 to this policy.

- **Do** report your concerns, as above; reports will be treated as confidential.
- **Do** persist if your concerns remain.
- **Do** retain or copy any relevant document(s). This holds documents for use in any subsequent investigation and avoids any documents being accidentally - or purposely – destroyed.
- **Don't** be afraid to seek advice from an appropriate person.
- **Don't** confront an individual or individuals with your suspicions.
- **Don't** discuss your concerns with colleagues or anyone else other than an appropriate person.
- **Don't** contact the police directly - that decision is the responsibility of the appropriate person and other senior University officers.
- **Don't** under any circumstances suspend anyone if you are a line manager without direct advice from Human Resources and other appropriate person(s).

6.2 Again, the University has a 'no retaliation' approach for people reporting reasonably held concerns and suspicions, and any retaliation against such people - including victimisation and deterring/preventing reporting - will be treated as a serious offence under the University's disciplinary processes. Equally, however, abuse of process by reporting malicious allegations will also be regarded as a disciplinary issue.

Any contravention of the no-retaliation approach should be reported through the University's Public Interest Disclosure Policy.

7.0 Fraud with Academic Implications

7.1 Fraud can often be associated with direct financial gain, such as procurement and invoicing fraud. However, in the University academic fraud is a further possibility, including fraud related to immigration, admissions, internships, examinations and awards.

Such a fraudulent activity could be very high-profile, with potentially significant consequences for the University. In such cases, it is again essential that an appropriate person is contacted at the earliest opportunity, together with other senior University officer(s), as deemed appropriate. As each case of this type is different, it is largely impossible to produce fully definitive guidance to follow.

Such a fraud may involve a number of stakeholders, including professional bodies, but decisions regarding their involvement generally remain the purview of senior University officers. To ensure that the investigation is not compromised, however, it is vital that the number of people aware of the investigation is kept to an absolute minimum. Notwithstanding, it should be recognised that some frauds of this nature will involve the police initiating their own investigation.

8.0 Associated Policies

8.1 University's Public Interest Disclosure Policy (Whistleblowing)
8.2 Prevention of Illegal Working Manual
8.3 Bullying and Harassment Policy
8.4 Code of Conduct Policy
8.5 Disciplinary Procedure
8.6 Grievance Policy
8.9 Procedure for Dealing with Breaches of Assessment Regulations – Academic Misconduct.

9.0 Responsibilities

9.1 Ultimate responsibility for this policy rests with the Board of Governors but the Vice-Chancellor and the Executive will ensure that this policy is applied effectively.

9.2 The prevention, detection and reporting of fraud and other forms of corruption are the responsibility of all those working for the University or under its control. All members of staff within the University are required to avoid any activity that might lead to, or suggest, a breach of this policy.

9.3 Any member of the University who breach this policy will face potential disciplinary action, which could result in dismissal for gross misconduct in the case of an employee, or expulsion from the University for students.

9.4 The University reserves the right to terminate any contractual relationship with contractors, agency or consultants if they breach this policy.

9.4 The University must include a 'statement of internal control' in its financial statements. The statement of internal control relates to arrangements for the prevention and detection of corruption, fraud, bribery and other irregularities. It must include an account of how the following principles of internal control have been applied:

a. Identifying and managing risk should be an ongoing process.
b. The approach to internal control should be risk-based, including an evaluation of the likelihood and impact.
c. Review procedures must cover business, operational and compliance risk as well as financial risk.
d. Risk assessment and internal control should be embedded in ongoing operations.
e. During the year the Audit and Risk Committee receive regular reports on internal control and risk.
f. The principal results of risk identification, risk evaluation and the management review of the effectiveness of the arrangements should be reported to and reviewed by the Audit and Risk Committee.

10.0 How to Raise a Concern

10.1 All members of the University are encouraged to raise concerns about any issue or suspicion or malpractice at the earliest possible stage. If an individual is unsure whether a particular act constitutes fraud, or if they have any other queries, these should be raised through the Business Risk Manager.

10.2 Alternatively, the matter can be raised in accordance with the University's Public Interest Disclosure Policy.

University list of appropriate persons and how to contact them

11.0 Operative

This policy was approved by the Audit and Risk Committee.

Appropriate Person	Name	Phone	Email
Chief Finance Officer (Money Laundering Nominated Officer)	Sally McGill	01782 292717	sally.mcgill@staffs.ac.uk
Chief Operating Officer (Governing Officer)	Ian Blach-ford	01785 353299	i.blachford@staffs.ac.uk
Head of Risk and Resilience (Fraud First Responder)	Clare Mayer	01782 294884	clare.mayer@staffs.ac.uk

Anti-bribery and Corruption Policy

Policy Coversheet

Name of Policy:	Anti-Bribery and Corruption Policy
Purpose of Policy:	To define how the University manages bribery and corruption
Intended Audience(s):	All Staff
Approval for this Policy given by:	Audit and Risk Committee
Last Review Date:	February 2025
Review Due Date: (3 years from last review)	February 2026
Individual responsible for Review:	Head of Risk and Resilience
Authorising Department:	Corporate Services

Anti-bribery and Corruption Policy

1.0 Policy Statement

1.1 The University is committed to the proper use of funds, both public and private. Therefore, it is essential that everyone associated with the University - including staff, students, employees, contractors and third-parties - are aware of the risk of bribery, corruption, theft and other activities involving dishonesty, in all its forms.

1.2 The University aims to reduce instances of bribery and corruption to the absolute practical minimum - and to also put in place arrangements that hold any bribery or corruption to a minimum level on an ongoing basis. The University's approach to bribery and corruption will be comprehensive, cost- effective and professional, using specialist expertise if, as and when required.

2.0 Definitions

2.1 Corruption can be defined as dishonest or fraudulent conduct, typically involving bribery.

Bribery can be defined as the offering, giving, receiving or soliciting of any item of value (money, goods, favours or other forms of recompense) to influence the actions of an official or other person in charge of a public or legal duty.

3.0 Anti-Bribery and Corruption Policy

3.1 The University is committed to the highest standards of integrity, probity and ethics in all its dealings - wherever they may take place and in whatever context. Bribery is both illegal and unethical, and brings with it the potential for criminal liability and severe penalties - at both University and individual level. The legislation is extensive and, crucially, the University's anti-bribery responsibilities do not end at the office door or campus gate. Those responsibilities potentially extend to any associated person, representative, agent, subsidiary, partnership or body engaged on University business.

3.2 The University has a zero-tolerance approach to bribery and serious action will be taken against anyone found to be involved in bribery, up to and including dismissal under the University's disciplinary processes. For associated persons, breach of this policy may result in contractual, legal and/or other sanction(s).

3.3 This policy applies to all University staff and students. It also applies to agency and self- employed workers working for the University, and all other persons associated with and acting for the University, whether directly or indirectly. This definition includes external members of University Committees, such as governors, representatives, agents, subsidiaries, individuals appointed as directors of any company, consultants, contractors and partners. To the fullest extent permissible by law, this policy shall apply in all jurisdictions in which the University operates.

3.4 It should be stressed that, in common with other Higher Education Institutions (HEIs), the University faces a range of bribery risks throughout its activities, operations and geographies. These risks include, but are not limited to, bribery in relation to admissions, examinations, awards, procurement, construction etc.

3.5 Policy statements

- The University values its reputation for ethical behaviour and recognises that any involvement in bribery is illegal and will reflect adversely on its image and reputation.
- The University prohibits the offering, giving, soliciting or the acceptance of any bribe in whatever form to, or from, any person or company (public or private) by anyone associated with the University.
- The University expects any person or company (public or private) associated with the University to act with integrity and without any actions that may be considered an offence within the meaning of the Bribery Act 2010.
- The University requires any potential breaches of this policy and bribery offers to be reported to the Head of Risk and Resilience
- The prevention, detection and reporting of bribery is the responsibility of everyone associated with the University.

4.0 The Bribery Act 2010 and other legislation

4.1 **The Bribery Act (2010)**
The Act came into force in July 2011. According to the Act, bribery is where someone requires, gives or promises financial (or other) advantage with the intention of inducing or rewarding improper performance. Improper performance is a key concept and generally means where an individual does not act in good faith, impartially and/or properly. The test of what is proper is based upon what a person in the UK would reasonably expect.

A typical example of improper performance could involve work being continually directed to a particular construction contractor at the expense of other qualified contractors as a result of bribery - work that has invariably been overpriced to allow for the bribery payments required.

Under the Act, there are two general forms of bribery where individuals are personally criminally liable:

- Offering, promising or giving of a bribe (either directly or indirectly) with the intent to induce a person to improperly perform a relevant function - known as active bribery.
- Requesting, agreeing to receive or accepting a bribe (either directly or indirectly) such that a relevant function is, or will be, improperly performed - known as passive bribery.

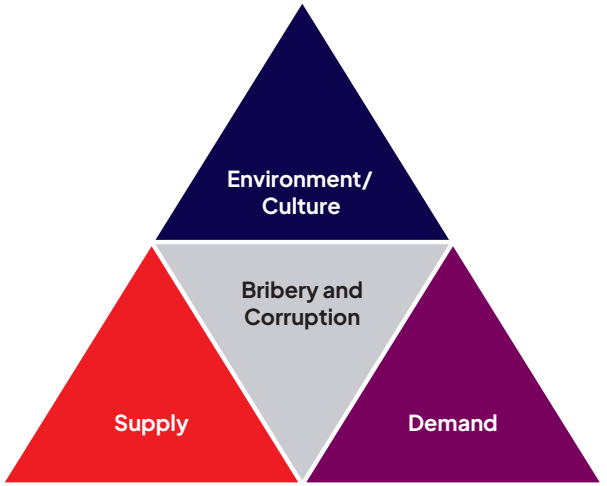
There are two other related offences:

- Bribing a foreign public official in order to obtain or retain business or an advantage to the conduct of business.
- Corporate liability where a body, such as a University, fails to prevent bribery. It is important to note that: so-called 'facilitation payments' - payments typically to government officials to facilitate special treatment, such as prioritisation in an approval process - are also bribes. The University does not offer or make, and shall not demand or accept, facilitation payments of any kind. Advice should be sought if required in order to distinguish between properly payable fees and disguised requests for facilitation payments. The timing of bribery payments - before, during and/or after a relevant function -does not affect the offence.

4.2 Overseas reach - The Bribery Act has extensive global reach and holds UK organisations liable for failing to implement adequate procedures sufficient to prevent such acts by those working for the University or on its behalf, no matter where in the world the act takes place.

4.3 Mitigation - There is a statutory defence against the Act if the University can demonstrate that it had in place appropriate adequate procedures designed to prevent bribery.

The 'Bribery Triangle', below, shows the three key drivers of bribery and corruption:



4.4 The University's Anti-Bribery and Corruption Policy is intended to directly mitigate its risk of bribery and corruption by impacting the three elements of the bribery triangle - by changing the organisational environment and culture, by removing/restricting the supply of money, goods, services and favours and/or reducing the demand for bribery. Reducing the demand for bribery, although clearly challenging, can be achieved in a number of ways including collaboratively creating a 'level playing field' or 'no bribery' approach in the higher education sector.

5.0 Anti-Bribery and Corruption Actions

5.1 **Risk Management**
Effective risk management lies at the very heart of this policy. Risk management is a crucial element of the University's overall governance process. It facilitates identification of the specific areas where the University does, or could, face bribery and corruption risks and allows mitigation plans, actions and protections to be put in place.

5.2 Areas of Risk
Whilst the University's high risks will undoubtedly change over time, the areas of continuing bribery high risk that will require enhanced levels of due diligence and caution will almost certainly include:

- Agents and intermediaries, particularly those who operate in jurisdictions where bribery is prevalent or endemic.
- Joint Ventures and consultancies, where the University could be held liable for any bribery or corruption committed by a third party with whom the University is associated by means of a joint venture or consultancy agreement.
- Contracts, particularly construction contracts where the values involved are likely to be high - and the industry has a perceived propensity for bribery.
- All aspects of procurement of services (particularly) and goods undertaken by the University.

Fraud can often be associated with direct financial gain, such as procurement and invoicing fraud. However, in the University/Higher Education sector, academic fraud is a further possibility, including fraud related to immigration, admissions, internships, examinations and awards.

Such a fraudulent activity could be very high-profile, with potentially significant consequences for the University. In such cases, it is again essential that an appropriate person is contacted at the earliest opportunity, together with other senior University officer(s), as deemed appropriate. As each case of this type is different, it is largely impossible to produce fully definitive guidance to follow.

Such a fraud may involve a number of stakeholders, including the police and professional bodies, but decisions regarding their involvement - generally - remain the purview of senior University officers. To ensure that the investigation is not compromised, however, it is vital that the number of people aware of the investigation is kept to an absolute minimum.

Notwithstanding, it should be recognised that some frauds of this nature will involve the police initiating their own investigation.

6.0 Financial Inducement, Gifts and Hospitality

6.1 Staff shall not accept any fee or financial inducement for work conducted as part of their University employment other than the pay and allowances to which they would normally be entitled from the University, in accordance with their contract of employment, supporting terms and conditions and the university's financial regulations.

6.2 Staff should not use University finances to purchase gifts for other members of staff, or external third parties.

6.3 **Gifts**

6.3.1 Gifts from external parties to University members of staff/governors should not be sought or encouraged. However, where a gift is received from an external party on an unsolicited basis, the following process should be followed:

- The recipient of the gift should declare this to the relevant role holder as indicated below:

Recipient of Gift	Line Manager/Approver
Chair of Board of Governors	Deputy Chair of the Board and Vice
All other Governors	Chair of the Board
Vice Chancellor	Chair of the Board
Executive	Vice Chancellor
Deans and Directors	Appropriate member of Executive
All other Staff	Appropriate Dean or Director

- Low value branded promotional items such as pens, calendars and diaries do not need to be declared and may be retained by the individual. A completed Gifts and Hospitality Form is not required.
- Other gifts such as chocolates, bottles of wine etc below the value of circa £25 may be accepted but the recipient should discuss with their line manager whether the gift should be raffled for charity purposes, shared with the team or personally retained. A completed Gifts and Hospitality Form is not required.

- Gifts over a value of circa £25 should be declared to the appropriate line manager/approver by the recipient. If the line manager/approver believes that the University, its reputation or staff members/governors will not be compromised by the acceptance of the gift; the gift may be approved and thus accepted.
- Where a gift is approved, the recipient should discuss with their line manager/approver whether the gift should be raffled for charity purposes, shared with the team or personally retained. The recipient and the line manager/approver must complete the Gifts and Hospitality Form and send this to the Clerk to the Board of Governors for formal recording in the Register of Gifts and Hospitality.

6.3.2 Gifts to members of staff from other University members of staff will not be covered by this policy. However, where the offering and receipt of gifts between staff members is a cause for concern, specifically in relation to their probity or conduct, this will be investigated in accordance with the University's Disciplinary Procedure. The same will apply for members of the Board of Governors.

6.4 **Hospitality**

6.4.1 Hospitality from external parties to the University members of staff and Governors should not be sought or encouraged. Examples of hospitality include sporting or social events unconnected with the individual's role. However, where hospitality is received on an unsolicited basis, from an external party, the following process should be followed:

- The recipient of the hospitality should declare this to the relevant role holder, in advance where practicable, as indicated below:

Recipient of Hospitality	Line Manager/Approver
Chair of Board of Governors	Deputy Chair of the Board and Vice
All other Governors	Chair of the Board
Vice Chancellor	Chair of the Board
Executive	Vice Chancellor
Deans and Directors	Appropriate member of Executive
All other Staff	Appropriate Dean or Director

- The hospitality will be approved, where the line manager/approver does not feel that the University, its reputation or staff members will be compromised and that it facilitates a legitimate business need.
- Where an offer of hospitality is approved, the recipient and the line manager/approver must complete the Gifts and Hospitality Form and this should be sent to the Clerk to the Board of Governors for formal recording in the Register of Gifts and Hospitality.
- If hospitality has been received and this has not been considered in advance, the hospitality must still be declared through the above route. Consideration will be given by the line manager/approver as to whether the hospitality could have been practicably approved in advance and whether the University, its reputation or staff members or Governors are, as a result, compromised and whether this served a legitimate business need. The line manager/approver must complete the Gifts and Hospitality Form and this should be sent to the Clerk to the Board of Governors for formal recording in the Register of Gifts and Hospitality. Where concerns exist regarding the probity of the individual(s) receiving the hospitality, this will be investigated in accordance with the Disciplinary Procedure.

6.5 Care must always be taken to ensure that whenever such hospitality or gifts are accepted, no obligation to the person or organisation offering the hospitality or gifts is created. If in doubt, please consult the Clerk to the Board of Governors.

6.6 The Gifts and Hospitality Form is available on WorkVivo or from the Clerk to the Board of Governors.

6.7 The Remuneration Committee of the Board of Governors will receive an annual report on the Gifts and Hospitality received by members of Executive.

7.0 Communication Responsibilities

7.1 Ultimate responsibility for this Policy rests with the Board of Governors but the Vice-Chancellor and Executive will ensure that this Policy is applied effectively.

7.2 The prevention, detection and reporting of bribery and corruption are the responsibility of all those working for the University or under its control. All members of staff within the University are required to avoid any activity that might lead to, or suggest, a breach of this Policy.

7.3 Any member of the University (staff and students) who breach this Policy will face disciplinary action, which could result in dismissal for gross misconduct in the case of an employee, or expulsion from the University for students.

7.4 The University reserves the right to terminate any contractual relationship with contractors, agenda or consultants if they breach this Policy.

8.0 How to raise a concern

8.1 All employees and others associated with the University are encouraged to report any concerns that they may have regarding potential breaches of this policy, including incidents relating to external agencies and third parties. This includes any instances where we may be the victim of attempted bribery.

8.2 The University is fully committed to ensuring that there is a safe and confidential method of reporting any suspected wrongdoing to nominated officers. The University's also permits employees, and anyone contractually associated with the University to raise concerns of malpractice in the University, and those involving partners or competitors.

8.3 Any allegations of misconduct under this policy within the jurisdiction the University will be taken very seriously. If appropriate, action may be taken under the University's disciplinary process. Attempted bribery or acceptance of a bribe may be considered as gross misconduct and, where it is considered that a criminal offence has occurred, the police may be informed.

University list of appropriate persons and how to contact them

Appropriate Person	Name	Phone	Email
Chief Finance Officer (Money Laundering Nominated Officer)	Sally McGill	01782 292717	sally.mcgill@staffs.ac.uk
Chief Operating Officer (Governing Officer)	Ian Blach-ford	01785 353299	i.blachford@staffs.ac.uk
Head of Risk and Resilience (Fraud First Responder)	Clare Mayer	01782 294884	clare.mayer@staffs.ac.uk

9.0 Operative

This policy was approved by the Audit and Risk Committee.

Appendix 1
International University Bribery Examples

Australia: Curtin University lecturer accepted bribes from students

"A former Curtin University lecturer has admitted accepting bribes and passing students who should have failed. Tuck Cheong Foong, 54, … increased the marks of two of his students who would otherwise have failed their units in Applied Science in Construction Management after one paid him $3000 and the other paid $1500. He also increased the mark on an assignment of a third student and gave him a pass mark on an assignment that had not been submitted. Foong had a long-term personal and professional connection with the student's father in Malaysia."

(Perth Now, 2013)

South Africa: Blade aims to cut corruption in University procurement

"South African higher education minister Blade Nzimande says his department is considering approaching the National Assembly to pass legislation … to curb corruption and nepotism in institutions. We are considering making a request for parliament to consider regulation on matters relating to the involvement of staff, students or council members in the supply chain in institutions."

(Sunday Times, 2011)

United Kingdom: University of Bath student jailed over tutor bribe bid

"A failing student who tried to bribe his tutor while carrying a loaded air pistol has been jailed for 12 months. Yang Li, 26, placed £5,000 in cash on the professor's table but when he was told to leave, the gun fell from his pocket. Li, who admitted bribery and possessing an imitation firearm, was also ordered to pay £4,800 in costs. The court heard the innovation and technology management masters student had arranged the meeting with his University of Bath professor on 23 November. Mark Hollier, prosecuting, said Li was awarded a 37% mark in his dissertation - three marks off the 40% needed to pass - and wanted to discuss his options."

(BBC, 2013)

Anti-Money Laundering Policy

Policy Coversheet

Name of Policy:	Anti-Money Laundering Policy
Purpose of Policy:	To define how the University manages Money Laundering
Intended Audience(s):	All Staff
Approval for this Policy given by:	Audit and Risk Committee
Last Review Date:	February 2025
Review Due Date: (3 years from last review)	February 2026
Individual responsible for Review:	Head of Risk and Resilience
Authorising Department:	

Anti-Money Laundering Policy

Introduction
Policy Aims

The University is committed to ensuring the highest standards of probity in all of its financial dealings. It will therefore ensure that it has in place proper, robust financial controls so that it can protect its funds and ensure continuing public trust and confidence in it. Some of those controls are intended to ensure that the University complies in full with its obligations not to engage or otherwise be implicated in money laundering or terrorist financing. This policy sets out those obligations, the University's response and the procedures to be followed to ensure compliance.

Implementation

The Chief Financial Officer is directly responsible to the Board of Governors for the implementation of this policy. As such, with the Board's full support, (s)he will ensure:

i) regular assessments of the University's money laundering and terrorist finance risks are conducted and relied on to ensure the effectiveness of this policy;

ii) appropriate due diligence is conducted, as a result of which risks relating to individual transactions are assessed, mitigated and kept under review;

iii) anti-money laundering and counter-terrorist finance training is delivered within the University, including training on this policy; and

iv) this policy is kept under review and up-dated as and when necessary and levels of compliance are monitored.

1. Certain functions under this policy are to be undertaken by a Nominated Officer. For the purposes of this policy, the Nominated Officer is the Chief Financial Officer and, in their absence, their deputy.

2. This policy applies to all staff who are engaged in financial transactions for or on behalf of the University. Any failures to adhere to this policy may be dealt with under the University's disciplinary or poor performance policies, as appropriate. Note that any such failures also expose the individual concerned to the risk of committing a money laundering offence.

What is Money Laundering?

3. Money laundering is the process by which the proceeds of crime are sanitised in order to disguise their illicit origins and are legitimised. Money laundering schemes come with varying levels of sophistication from the very simple to the highly complex. Straightforward schemes can involve cash transfers or large cash payments whilst the more complex schemes are likely to involve the movements of money across borders and through multiple bank accounts. Money laundering schemes typically involve three distinct stages:

i) placement – the process of getting criminal money into the financial system;

ii) layering – the process of moving the money within the financial system through layers of transactions; and

iii) integration – the process whereby the money is finally integrated into the economy, perhaps in the form of a payment for a legitimate service.

Money Laundering Warning Signs or Red Flags

4. Payments or prospective payments made to or asked of the University can generate a suspicion of money laundering for a number of different reasons. For example:

i) large cash payments;

ii) multiple small cash payments to meet a single payment obligation;

iii) payments or prospective payments from third parties, particularly where

a. there is no logical connection between the third party and the student, or

b. where the third party is not otherwise known to the University, or

c. where a debt to the university is settled by various third parties making a string of small payments;

iv) payments from third parties who are foreign public officials or who are politically exposed persons ("PEP");

v) payments made in an unusual or complex way;

vi) unsolicited offers of short-term loans of large amounts, repayable by cheque or bank transfer, perhaps in a different currency and typically on the basis that the University is allowed to retain interest or otherwise retain a small sum;

vii) donations which are conditional on particular individuals or organisations, who are unfamiliar to the University, being engaged to carry out work;

viii) requests for refunds of advance payments, particularly where the University is asked to make the refund payment to someone other than the original payer;

ix) a series of small payments made from various credit cards with no apparent connection to the student and sometimes followed by chargeback demands;

x) the prospective payer wants to pay up-front a larger sum than is required or otherwise wants to make payment in advance of them being due;

xi) prospective payers are obstructive, evasive or secretive when asked about their identity or the source of their funds or wealth;

xii) prospective payments from a potentially risky source or a high-risk jurisdiction;

xiii) the payer's ability to finance the payments required is not immediately apparent or the funding arrangements are otherwise unusual.

Money Laundering - The Law

5. The law concerning money laundering is complex and is increasingly actively enforced. It can be broken down into three main types of offences:

i) the principal money laundering offences under the Proceeds of Crime Act 2002;

ii) the prejudicing investigations offence under the Proceeds of Crime Act 2002; and

iii) offences of failing to meet the standards required of certain regulated businesses, including offences of failing to disclose suspicions of money laundering and failing to comply with the administrative requirements of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.

The Principal Money Laundering Offences

6. These offences, contained in sections 327, 328 and 329 Proceeds of Crime Act 2002, apply to any property (e.g. cash, bank accounts, physical property, or assets) that constitutes a person's benefit from criminal conduct or any property that, directly or indirectly, represents such a benefit (in whole or partly) where the person concerned knows or suspects that it constitutes or represents such a benefit. Any property which meets this definition is called criminal property. It is a crime, punishable by up to fourteen years imprisonment, to:

i) conceal, disguise, convert or transfer criminal property or to remove it from the United Kingdom;

ii) enter into an arrangement that you know or suspect makes it easier for another person to acquire, retain, use or control criminal property; and

iii) acquire, use or possess criminal property provided that adequate consideration (i.e. proper market price) is not given for its acquisition, use or possession.

7. University staff can commit these offences when handling or dealing with payments to the University: if they make or arrange to make a repayment, they risk committing the first two offences, and if they accept a payment, they risk committing the third offence.

Defences

8. In all three cases, they will have a defence if they made a so-called authorised disclosure of the transaction either to the Nominated Officer or to National Crime Agency and the National Crime Agency does not refuse consent to it.

Failure to Disclose Offence

9. It is a crime, punishable by up to five years imprisonment, for a Nominated Officer who knows or suspects money laundering or who has reasonable grounds to know or suspect it, having received an authorised disclosure not to make an onward authorised disclosure to the National Crime Agency as soon as practicable after (s) he received the information.

10. At paragraph 32 below, this policy sets out how such disclosures are to be made.

The Offence of Prejudicing Investigations / Tipping-Off

11. The purpose of making an authorised disclosure to the National Crime Agency is to allow it to investigate the suspected money laundering so it can decide whether to refuse consent to the transaction. That investigation would be compromised if the person concerned (or indeed anyone else) were to be told that an authorised disclosure had been made. To prevent this happening section 342 Proceeds of Crime Act 2002 provides that it is a crime, punishable by up to five years imprisonment, to make a disclosure which is likely to prejudice the money laundering investigation. University staff can commit this offence if they tell a person an authorised disclosure has been made in their case. At paragraph 35 below, this policy requires authorised disclosures to be kept strictly confidential.

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017

12. These regulations are aimed at protecting the gateway into the financial system. They apply to a range of businesses all of which stand at that gateway. They require these businesses to conduct money laundering risk assessments and to establish policies and procedures to manage those risks. Businesses to which the regulations apply are specifically required to conduct due diligence of new customers, a process known as "Know your Customer" or "KYC". There are criminal sanctions, including terms of imprisonment of up to two years, for non-compliance. Whilst the University is not covered by the regulations in its work as a provider of education, the regulations provide a guide to the management of risk in handling money and due diligence is at the heart of the University's approach in this policy to managing risk.

13. To the extent that the University is regulated by the Financial Conduct Authority for part of its business, it must comply with Money Laundering Regulations (and a separate, more detailed policy sets out the university's approach here).

Terrorist Finance
The Principal Terrorist Finance Offences

14. Whereas money laundering is concerned with the process of concealing the illegal origin of the proceeds from crime, terrorist financing is concerned with the collection or provision of funds for terrorist purposes. The primary goal of terrorist financers is to hide the funding activity and the financial channels they use. Here, therefore, the source of the funds concerned is immaterial, and it is the purpose for which the funds are intended that is crucial.
15. Payments or prospective payments made to or asked of the University can generate a suspicion of terrorist finance for a number of different reasons, but typically might involve a request for a payment, possibly disguised as a repayment or re-imbursement, to be made to an account in a jurisdiction with links to terrorism.
16. Sections 15 to 18 Terrorism Act 2000 create offences, punishable by up to 14 years imprisonment, of:

i) raising, possessing or using funds for terrorist purposes;
ii) becoming involved in an arrangement to make funds available for the purposes of terrorism; and
iii) facilitating the laundering of terrorist money (by concealment, removal, transfer or in any other way).

17. These offences are also committed where the person concerned knows, intends or has reasonable cause to suspect that the funds concerned will be used for a terrorist purpose.
18. In the case of facilitating the laundering of terrorist money, it is a defence for the person accused of the crime to prove that they did not know and had no reasonable grounds to suspect that the arrangement related to terrorist property.
19. Section 19 Terrorism Act 2000 creates an offence, punishable by up to five years imprisonment, where a person receives information in the course of their employment that causes them to believe or suspect that another person has committed an offence under sections 15 to 18 of Terrorism Act 2000 and does not then report the matter either directly to the police or otherwise in accordance with their employer's procedures. This policy sets out those procedures at paragraph 32 below.

The Offence of Prejudicing Investigations

20. Section 39 Terrorism Act 2000 creates an offence, punishable by up to five years imprisonment, for a person who has made a disclosure under section 19 Terrorism Act 2000 to disclose to another person anything that is likely to prejudice the investigation resulting from that disclosure. At paragraph 35 below, this policy requires disclosures under the Terrorism Act 2000 to be kept strictly confidential.

OUR PROCEDURES
Overview

21. The University will:

i) conduct an annual risk assessment to identify and assess areas of risk money laundering and terrorist financing particular to the University;
ii) implement controls proportionate to the risks identified;
iii) establish and maintain policies and procedures to conduct due diligence on funds received;
iv) review policies and procedures annually and carry out on-going monitoring of compliance with them;
v) appoint a Nominated Officer to be responsible for reporting any suspicious transactions to the National Crime Agency;
vi) provide training to all relevant members of staff, including temporary staff, on joining the University, and provide annual refresher training; and
vii) maintain and retain full records of work done pursuant to this policy.

The University's Risk Assessment, Continuous Review and Accountability

22. At least once a year, and more frequently if there is a major change in circumstances, the Chief Financial Officer will:

i) conduct an assessment of money laundering and terrorist finance risk in the University's work;
ii) review and, if necessary, revise this policy in light of that risk assessment;
iii) review and, if necessary, revise the University's arrangements for ensuring compliance with this policy so that resources are targeted to the areas of greatest risk; and
iv) report to the Board on all aspects of this policy, including its implementation.

23. In order to facilitate the review and accountability functions, the Chief Financial Officer will ensure:

i) the availability of appropriate management information to permit effective oversight and challenge; and
ii) the maintenance and retention of full records of work done under this policy.

24. In conducting the assessment of money laundering and terrorist financing risk arising from the University's work and funding activity, the Chief Financial Officer/ Bursar will have regard to the University's experiences and to any lessons learned in applying this policy. (S)/he will also take into account any guidance or assessments made by the UK government, law enforcement and regulators, including the Charity Commission, the Office for Students and the Financial Conduct Authority. (S)he may also have regard to reports by non-governmental organisations and commercial due diligence providers.

Transaction Due Diligence

25. Due diligence is the process by which the University assures itself of the provenance of funds it receives and that it can be confident that it knows the people and organisations with whom it works. In this way the University is better able to identify and manage risk. Due diligence should be carried out before the funds are received. Funds must not be returned before due diligence has been reviewed.
26. In practical terms this means:
i) identifying and verifying the identity of a payer or a payee, typically a student or a donor;
ii) where the payment is to come from or to be made by a third party on behalf of the student or donor, identifying and verifying the identity of that third party;
iii) identifying and verifying the source of funds from which any payment to the University will be made; and
iv) identifying and in some circumstances verifying the source of wealth from which the funds are derived.
27. Source of funds refers to where the funds in question are received from. The most common example of a source of funds is a bank account. Source of wealth refers to how the person making the payment came to have the funds in question. An example of a source of wealth is savings from employment.
28. Guidance on how to do this when accepting payments from students is at Annexes 1 and 2.

Transaction Risk Assessment

29. Having completed its due diligence exercise, the University will assess the money laundering and terrorist finance risk associated with the proposed transaction.
30. Where the case falls into the category of case described in Annex 1 as suspicious or the member of staff dealing with the case otherwise considers there is a suspicion of money laundering or terrorist finance, (s)he must report the case as soon as practicable, by email, to the Nominated Officer on a Form 1, which is to be found at Annex 2.

31. The Nominated Officer will consider the report and will decide:
i) whether or not to accept or to make the proposed payment;
ii) whether or not to make an authorised disclosure to the National Crime Agency; and
iii) whether or not to make a disclosure under the Terrorism Act 2000.
32. The Nominated Officer will record in writing the reasons for their decision and retain that record centrally. Information that an authorised disclosure has been made must never be kept on the file relating to the person concerned.
33. Risk assessments relating to individuals and authorised disclosures are to be kept strictly confidential and should not be discussed within the finance department except on a strict need-to-know basis. No member of staff may reveal to any person outside the finance department, including specifically the student or third party funder in question, that an authorised disclosure or a disclosure under the Terrorism Act 2000 has been made.

Monitoring

34. The Chief Financial Officer will devise and implement arrangements to ensure that compliance with this policy is kept under continuous review through regular file reviews, including reviews of due diligence and risk assessment, and reports and feedback from staff. Internal audit may be called upon to assist in monitoring effective implementation of this policy.
35. To enable monitoring to be conducted and compliance with this policy to be evidenced, the University will retain all anti-money laundering and counter-terrorist finance records securely for a period of at least five years.

Training

36. On joining the University any staff whose duties will include undertaking a finance function will receive anti-money laundering training as part of their induction process.
37. All staff undertaking a finance function will receive annual refresher anti-money laundering and counter-terrorist finance training.
38. The University's anti-money laundering and counter-terrorist financing training will include the applicable law, the operation of this policy and the circumstances in which suspicions might arise.
39. The University will make and retain for at least five years records of its anti-money laundering training.

11.0 Contacts

University list of appropriate persons and how to contact them

Appropriate Person	Name	Phone	Email
Chief Finance Officer (Money Laundering Nominated Officer)	Sally McGill	01782 292717	sally.mcgill@staffs.ac.uk
Chief Operating Officer (Governing Officer)	Ian Blach-ford	01785 353299	i.blachford@staffs.ac.uk
Head of Risk and Resilience (Fraud First Responder)	Clare Mayer	01782 294884	clare.mayer@staffs.ac.uk

12.0 Operative

12.1 This policy was approved by the Audit and Risk Committee.

Appendix 1
Risk factors re. possible money laundering

It is not possible to give a definitive list of ways to spot money laundering or how to decide whether to make a report to the MLNO. The following are types of risk factors which may, either alone or collectively, suggest the possibility of money laundering activity.

- A new customer, business partner or sponsor not known to the University.
- A secretive person or business e.g. that refuses to provide requested information without a reasonable explanation.
- Payment of any substantial sum in cash (over £10,000).
- Concerns about the honesty, integrity, identity or location of the people involved.
- Involvement of an unconnected third party without a logical reason or explanation.
- Overpayments for no apparent reason.
- Absence of any legitimate source for the funds received.
- Significant changes in the size, nature, frequency of transactions with a customer thatis without reasonable explanation.
- Cancellation, reversal or requests for refunds of earlier transactions.
- Requests for account details outside the normal course of business.
- A history of poor business records, controls or inconsistent dealing.

Any other facts which tend to suggest that something unusual is happening and give reasonable suspicion about the motives of individuals.

Appendix 2
Suspected Money Laundering - Report to the MLNO

From:

School/Department:

Contact Details: email:

Phone:

DETAILS OF SUSPECTED OFFENCE

- Name(s) and address(es) of person(s) involved including relationship with the University.
- Nature, value and timing of activity involved.
- Nature of suspicions regarding such activity.
- Provide details of any investigation undertaken to date.
- Have you discussed you suspicions with anyone and if so on what basis.
- Is any aspect of the transaction(s) outstanding and requiring consent to progress.
- Any other relevant information that may be useful.

Signed:

Date:

Appendix 3
MLNO Report

To be completed by the MLNO

Date Report Received:

Date Receipt of report acknowledged:

CONSIDERATION OF DISCLOSURE

- Further Action Required.
- Are there reasonable grounds for suspicion requiring a report be made to NCA
- If YES: Confirm date of report to NCA: .....

Address: UKFIU, PO Box 8000, London SE11 5EN
Or by fax to 0207 238 8286

Or online via the website:
https://www.ukciu.gov.uk/(sct3dnqovty1ocisb5hzfy45)/saronline.aspx

- Any further details
- Is consent required from NCA to any on-going transactions?
- If YES: confirm details and instructions
- Date consent received: .....
- Date consent given to staff: .....
- IF NO: Confirm reason for non-disclosure
- Date consent given to staff: .....

Signed:

Date:

PUBLIC INTEREST DISCLOSURE POLICY AND PROCEDURES

1.0 Introduction

1.1 Staffordshire University has a duty to conduct affairs in a responsible and transparent way and to take account of the requirements of its funding bodies for the proper use of public funds and of the standards required in public life.

1.2 Where an individual discovers information which they reasonably believe shows malpractice or impropriety within the organisation then this information should be disclosed without fear of reprisal, and may be made independently of line management.

1.3 The Board of Governors has overall responsibility for this policy and procedure.

1.4 This policy does not form part of any member of staff's contract of employment and the University may amend it at any time.

2. Scope of the Policy

2.1 This policy applies to University staff, including 'workers', as they are referred to in the Public Interest Disclosure Act 1998 ('the Act'). This policy does not apply to students or to members of the general public.

2.2 The policy is intended to cover disclosures of information within the University which are in the public interest and which the individual making the disclosure reasonably believes tend to show one or more of the following has occurred, is occurring, or is likely to occur:

- financial malpractice including fraud
- a miscarriage of justice
- failure to comply with a legal obligation (this may include, for example, obligations such as freedom of speech and academic freedom, obligations under the Equality Act, or compliance with the University's regulations)
- danger to the health or safety of any individual
- damage to the environment
- criminal offence
- and/or deliberate concealment of information tending to show any matter falling within any of the above.

2.3 This policy and procedure is not designed to:

- challenge financial or business decisions properly taken by the University;
- consider any matters relating to a member of staff's employment or work, or a student's study or personal circumstances which should be, are being, or have been addressed, under the University's separate procedures, for example staff discipline, staff grievance, bullying and harassment, student complaints
- to consider any matters which fall outside of those outlined in 2.2 above and/or under other University procedures.

2.4 If you are uncertain whether something is within the scope of this policy, you should seek advice from the Clerk to the Board of Governors, whose contact details are at the end of this policy. If the matter refers to the Clerk to the Board, you should seek advice from the Vice Chancellor and Chief Executive or Chair of the Audit and Risk Committee as outlined in Section 5 of this policy.

3. Safeguards

3.1 Protection

3.1.1 Anyone raising a genuine concern in accordance with this policy is entitled to not be subjected to any detriment as a result of having done so. If an individual reasonably believes that they have suffered such treatment, the individual should raise it formally using the University's Grievance Procedure.

3.1.2 The individual will also be protected if they make the disclosure to an appropriate person/body outside the University, such as a regulator or professional body or an MP. A list of the relevant prescribed people and bodies for this purpose and the areas for which they are responsible is available on the GOV.UK website at: https://www.gov.uk/government/publications/blowing- the-whistle-list-of-prescribed-people-and-bodies--2

3.1.3 The University will not tolerate any threat, retaliatory action or harassment against an individual because they have raised a concern. Any person involved in such conduct may be subject to disciplinary action and in some cases will be liable to a claim for compensation brought against them personally.

3.1.4 Independent advice on the protection offered to workers who disclose public interest concerns is available from Protect. This charity offers free, impartial and confidential advice and guidance to potential whistleblowers. Its details are Protect, The Green House. 244 – 254

Cambridge Heath Road, London, E2 9DA, (Email: whistle@protect-advice.org.uk, Tel: 020 3117 2520).

3.2 Confidentiality

3.2.1 The University will treat all disclosures of information raised in accordance with this policy in a confidential and sensitive manner. The identity of the individual making the allegation may be kept confidential so long as it does not hinder or frustrate any investigation. However, the investigation process may reveal the source of the information and the individual making the disclosure may need to provide a statement and engage in the process as part of the evidence required.

3.3 Anonymous Allegations

3.3.1 This University encourages individuals to put their name to any disclosures they make. Concerns expressed anonymously are generally more difficult to investigate and whether they will be considered is at the discretion of the University.

3.3.2 In exercising this discretion, the factors to be taken into account will include:

- the seriousness of the issues raised;
- the credibility of the concern; and
- the likelihood of confirming the allegation from alternative credible sources.

3.4 Untrue Allegations

3.4.1 If an individual makes a disclosure of information in the reasonable belief that it tends to show one or more of the items in paragraph 2.2 above and it is in the public interest, even if this is found not to be the case (whether at the outset, by a subsequent investigation or otherwise), no action will be taken against that individual. If, however, an individual makes a disclosure of information, which is found to be malicious and/or vexatious, disciplinary action may be taken against the individual concerned.

4. Procedures

4.1 Initial Step

4.1.1 The University strongly encourages any individual to use the procedure outlined at Section 4 and seek appropriate advice prior to raising complaints externally.

4.1.2 The University hopes that in many cases an individual will be able to raise any concerns with their line manager in the first instance, verbally or in writing. They may be able to agree to a way of resolving the individual's concern quickly and effectively.

4.1.3 However, where the matter is more serious, the individual considers that their line manager has not addressed their concern, or the individual would prefer not to raise it with their line manager for any reason, then they should make the disclosure to the Designated Person, who is the Clerk to the Board of Governors. If, however, the disclosure is about the Clerk to the Board of Governors then the disclosure may be made to the Vice-Chancellor or the Chair of the Audit and Risk Committee of the Board of Governors. Contact details are listed in Section 5 of this procedure.

4.1.4 The individual will generally need to provide the following information as a minimum:

- the details of the concern and why the individual believes it to be true; and
- the background and history of the concern (giving relevant dates where possible).

4.1.5 The University may ask the individual for further information about the concern raised, at any stage of the procedure and the individual should respond to the request as promptly and comprehensively as possible.

4.1.6 If the disclosure is received in writing, then a written acknowledgement will normally be provided within five working days.

4.2 Process

4.2.1 The Designated Person, or their nominee (or Vice-Chancellor or the Chair of the Audit and Risk Committee of the Board of Governors if the disclosure is about the Designated Person), will consider the information made available to them. Normally within two weeks of the concern being received in accordance with paragraphs 4.1.3 and 4.1.4 above, they will decide whether they consider that there is a prima facie case that should be considered further in accordance with this policy or not. If they consider that it should, they will decide whether:

- to investigate the matter internally or externally;
- to refer the matter to the Police or other appropriate authority; and/or
- to take other action as deemed appropriate.

4.2.2 If an investigation is to be commenced, the Designated Person will then decide :
- who should undertake the investigation;
- the procedure to be followed; and
- the scope of the investigation.

4.2.3 Investigations should not be carried out by the person who will have to reach a decision on the matter.

4.2.4 Normally within a week of the decision by the Designated Person, the Designated Person will then commission the investigation to commence.

4.3 Investigation and Next Steps

4.3.1 Any investigation will be conducted as sensitively and speedily as possible. This should normally be within one month of the concern being received in accordance with paragraphs 4.1.3 and 4.1.4 above.

4.3.2 The party instructed to undertake the investigation (the "Investigating Officer") will arrange a meeting as soon as possible to discuss the concern raised by the individual. The individual may bring a colleague or trade union representative to the meeting. The companion must respect the confidentiality of the disclosure and any subsequent steps undertaken.

4.3.3 Save for certain circumstances where it may not be appropriate (for example, when an external authority requests the University not to), where a disclosure is made, the person or persons against whom the disclosure is made will be informed, provided with the evidence supporting it and will be allowed to respond as part of any investigation.

4.3.4 Once the investigation has been completed, a copy of the report will be sent to the Designated Person, or their nominee, who will retain such reports in accordance with any applicable document retention requirements. Normally within a month of the investigation being completed, the Designated Person, or their nominee, will decide whether further action should be taken. This may include the commencement of a formal procedure, other appropriate action and /or no further action.

4.3.5 In some instances, it might be necessary to refer the matter to an external authority for further investigation.

4.4 Feedback

4.4.1 Where it is not prevented due to the confidentiality, or particular sensitivity and /or other reasons relating to the matter, the individual complainant and/or accused will normally be given an update on the progress of the matter and details of the outcome of the investigation or any further action taken as a result. Whilst there is no entitlement to receive any such information, the individual complainant and /or accused should treat any information they do receive as confidential. Neither the complainant nor the accused has any right to appeal against the findings or any decision made in accordance with this Policy. The Chair of the Audit and Risk Committee will ensure that the Chair of the Board of Governors is kept reasonably informed, as they deem appropriate.

4.5 Reporting

4.5.1 Reporting to those other than the complainant and the accused (which are addressed in paragraph 4.4.1 above) on the instigation, progress, outcomes or further action of any investigation will depend on the nature of the concern raised and the resulting findings. It may include internal or external reporting. The Designated Person or nominee will normally (if they determine it to be appropriate in the circumstances) inform the Chair of the Audit and Risk Committee of the instigation of the procedure and provide updates. In all cases a summary report of the outcomes of any investigation will be made to the Audit and Risk Committee. Any report made will be in accordance with applicable data protection legislation and any safeguards necessary to maintain the integrity of the procedure undertaken.

5.0 Contacts

5.1 The University website address is www.staffs.ac.uk
5.2 The Chair of the Audit and Risk Committee of the Board of Governors is Jonathan Chapman (email jonathan.chapman@staffs.ac.uk)
5.3 The Clerk to the Board of Governors is Ian Blachford, also the Chief Operating Officer (email i.blachford@staffs.ac.uk)
5.4 The Vice Chancellor and Chief Executive is Professor Martin Jones (email martin.jones@staffs.ac.uk).

6. Approval

6.1 The equality impact of this policy has been taken into account during the development of this policy and all protected characteristics have been considered as part of the Equality Analysis undertaken.
6.2 This policy was reviewed and updated by the Audit and Risk Committee on 12th February 2025.

University of Staffordshire
College Road
University Quarter
Stoke-on-Trent
ST4 2DE

www.staffs.ac.uk

100266E