

Fraud Risk Management Policy

Contents

1. Introduction	1
2. Policy Statement	1
3. Relationship to the University Values and Other University Policies	2
4. Fraud Control Strategy	2
A. Roles and Responsibilities	3
B. Fraud Risk Management Framework.....	6
C. Fraud Risk Assessment	6
D. Fraud Prevention and Detection Controls	6
5. Fraud Reporting	7
6. Fraud Response Procedures.....	7
7. Monitoring of Fraud Policy Effectiveness	8
8. Training	8
9. Policy Non-Compliance	8
10. Policy Review.....	8
Appendix 1 – Sample Definitions.....	9
Appendix 2 – Indicators and Warning signs of fraud	10
Appendix 3 – Examples of controls to prevent and detect fraud	10

Document History

Title:	Fraud Risk Management Policy	
Policy Owner	Chief Strategy and Finance Officer	
Version	v1.2	
Approved By	Senior Leadership Team	05.11.24
	Audit and Risk Committee	20.01.25
Next Review Date	January 2028	

1. Introduction

The purpose of this policy is to support Ulster University in effectively managing the risk associated with fraud and provide the guiding principles used to set direction on the identification, assessment, mitigation, monitoring and reporting of fraud in the University.

Ulster University is committed to fraud prevention, detection, and deterrence and will address not just internal fraud risks i.e. fraud perpetrated by parties within the organisation, but also external fraud risks such as fraud perpetrated on the organisation by outside parties including identity theft, ransomware, data breaches, and a wide range of corruption schemes that continue to evolve.

The University's activities require significant funds, and as a charity with significant income derived from public funds, the University is accountable to a wide range of stakeholders for the use and management of those funds. It is the responsibility of all University officers and staff to ensure that University funds and resources are used honestly and correctly, and to report any circumstances which may indicate their improper use. This responsibility aligns to the University Values of Integrity, Collaboration, Inclusion and Enhancing Potential, with this policy building on these values in terms of the approach and channels to be used to report and manage incidents of fraud.

This policy is aligned with the Committee of Sponsoring Organisations of the Treadway Commission (COSO), Internal Control Framework and Principles on Fraud Risk Management. It also aligns to obligations placed on the University in the Financial Memorandum/ Partnership Agreement between the University and its funding Department, DfE.

2. Policy Statement

The University has defined its Risk Appetite and determined it is risk averse to any exposure to fraudulent activities. Therefore, this policy establishes management's framework of internal controls for the prevention and detection of fraud and theft within the University, as well as protocols for conducting investigations.

This Policy applies to any attempted, suspected or actual fraudulent activities or theft involving students, employees, as well as the Council/Committee Co-Optees, and third parties with a business relationship with the University.

Fraud comprises:

- Attempted Fraud: Attempted fraud occurs when someone engages in deceptive or dishonest behaviour with the intent to commit fraud, but their efforts are unsuccessful.
- Suspected Fraud: Suspected fraud refers to situations where there are indications or red flags suggesting fraudulent activity, but it hasn't been conclusively proven.
- Actual Fraud: Actual fraud involves a successful deceptive act with the intent to deceive.

Any employee or student may submit a report relating to fraud without fear of dismissal or victimisation. Investigations will be conducted without regard to the suspected employee's or third party's length of service, position/title, or relationship to the University. Decisions to prosecute or refer to regulatory agencies and/or law enforcement will be made by the Fraud and Theft Response Team which comprises:

- Chief Strategy & Finance Officer (Chair)
- Chief People Officer (Deputy Chair)
- Director of Risk & Resilience
- Director of Finance
- Director of People and Culture (Partnerships and Services)
- Other co-opted individuals as deemed necessary.

For cases of non-academic student fraud, following investigation and where appropriate, cases will be referred to the Student and Academic Affairs Team, who will determine if/when the case is referred to the Office of the University Secretary for consideration under the approved Student Conduct Ordinance.

The [Fraud Act 2006](#) states that a person is guilty of fraud if they are in breach of any of the sections listed below, (which provide for different ways of committing the offence):

- **Fraud by false representation:**
 - A person is in breach of this section if he/she:
 - intends, by making the representation
 - (i) to make a gain for himself or another, or
 - (ii) to cause loss to another or to expose another to a risk of loss
- **Fraud by failing to disclose information:**
 - A person is in breach of this section if he/she:
 - (a) dishonestly fails to disclose to another person information which he is under a legal duty to disclose, and
 - (b) intends, by failing to disclose the information
 - (i) to make a gain for himself or another, or
 - (ii) to cause loss to another or to expose another to a risk of loss
- **Fraud by abuse of position:**
 - A person is in breach of this section if he/she:
 - (a) occupies a position in which he is expected to safeguard, or not to act against, the financial interests of another person,
 - (b) dishonestly abuses that position, and
 - (c) intends, by means of the abuse of that position
 - (i) to make a gain for himself or another, or
 - (ii) to cause loss to another or to expose another to a risk of loss

Management is expected to be familiar with the types of fraud that could occur within their specific areas of responsibility and report any suspected or known instances of fraud within the University. The appendices outline the main types of fraud which could occur in the University, warning signs and existing controls. The reporting requirements to DfE are outlined in Appendix 1 in the [Fraud and Theft Response Procedure](#).

Theft is defined (per the Theft Act (Northern Ireland) 1969 as 'Dishonestly appropriating the property of another with the intention of permanently depriving them of it, immaterial of whether the appropriation is made with a view to gain. This may include the removal or misuse of funds, assets or cash.'

3. Relationship to the University Values and Other University Policies

The Council and Management have adopted this Fraud Risk Management Policy as a complement to the University's Values of Integrity, Collaboration, Inclusion and Enhancing Potential and other University policies designed to foster and promote the highest standards of ethical practices across the University. Employees at every level have responsibility for ensuring that the University's activities align with University Values as well as other policies designed to ensure compliance with laws, rules, and regulations in the jurisdictions in which the University operates. These include the following:

- [Anti-Bribery Act Guidance](#)
- [Anti-Money Laundering Policy](#)
- [Disciplinary Procedures \(Staff\)](#)
- [Gifts, Gratuities and Hospitality Policy](#)
- [P Card policy](#)
- [Procedure for the Investigation of Allegations of Research Misconduct](#)
- [Raising Concerns \(Whistleblowing\) Policy](#)
- [Student Conduct Ordinance](#)
- [Travel, Expenses and Hospitality Policy](#)

4. Fraud Control Strategy

A. Roles and Responsibilities

All University staff, regardless of their level, are responsible for helping deter and defend the University from fraud and theft. The section below highlights the roles and responsibilities within the University's Fraud Risk Management Framework.

(i) Council and Audit and Risk Committee

To set the appropriate tone for the University, the Council is responsible for ensuring that management designs an effective Fraud Risk Management Framework. The Council has delegated this responsibility to the Audit and Risk Committee. The Audit and Risk Committee should:

- Periodically review and approve the University's Fraud Risk Management Policy, as well as other applicable University policies and procedures designed to help mitigate fraud risk.
- Receive assurances from the External Auditor and Internal Audit regarding assessment of the risk of fraud by management, including the risk of management's override of controls, and ensuring that controls are designed and functioning to deter, prevent, and detect fraud by management.
- Be fully informed about instances of fraud that occur within the University involving senior-level employees or employees about whom significant internal control issues are uncovered, together with progress on the related investigation and lessons learned.
- Ensure that the Internal and External Auditors, and appropriate authorities, have been informed of cases where appropriate.

(ii) Senior Leadership Team (SLT)

Management has overall responsibility for the design and implementation of the University's fraud risk management Framework, including:

- Ensuring that fraud is addressed in the University's strategic objectives and risk assessment activities.
- Appointing the fraud control officer, who has overall responsibility for the coordination and implementation of the University's fraud risk management Framework as well as reporting to the Audit and Risk Committee about fraud risk matters.
- Identifying and assigning staff responsible for anti-fraud control activities, as outlined in the Fraud Risk Register and associated mitigation plans, and maintaining records that verify that those processes and controls have been properly executed.
- Providing defined, proactive processes and control activities to deter, prevent, and detect fraud.
- Implementing internal controls designed to prevent and/or detect fraud within each department and faculty.
- Promote understanding of, training on, and compliance with this Fraud Risk Management Policy, and other related corporate policies listed in section 3 above.
- Maintaining an open-door policy and other mechanisms to report fraud and misconduct.

(iii) All Managers

- Ensuring fraud control activities, both preventative and detective, are identified, developed, implemented and monitored.
- Facilitating new employee orientation and other employee training activities.
- Escalating issues involving potential fraud reported by management and employees.
- Participating in management's fraud risk assessment activities.

(iv) Risk Management Committee (RMC)

- Ensuring that fraud risk has been considered as part of management's strategic objectives and risk assessment activities.
- Overseeing management's fraud risk assessment activities.
- Periodically review the fraud risk register.
- Ensuring that management has assigned sufficient resources to execute fraud risk management

activities.

- Monitoring management's reports on fraud risks, policies, and control activities.

(v) People and Culture

The People and Culture directorate assists management and employees by supporting key anti-fraud control activities including:

- Supporting internal fraud investigation activities, as needed.
- Coordinating disciplinary or corrective action, if deemed necessary by the Fraud and Theft Response Team.
- Providing access to and monitoring of training via the Learning Management System.

(vi) Internal Audit

The internal audit function (outsourced) provides independent, objective assurance and consulting activities to the University. The Internal Audit function provides:

- Assurance that the University's processes are adequate to identify and monitor significant risks relating to fraud;
- Confirmation of the effective and efficient operation of the established internal controls;

The responsibility for the prevention, detection and resolution of fraud lies with Management. This responsibility is addressed through the implementation and continued operation of an effective system of internal control.

Internal Audit has a responsibility to ensure that the audit plan and methodology takes appropriate account of the possibility of fraud. Internal Audit may assist the University with investigations in accordance with the University's Fraud Risk Management Policy. In these circumstances, the Internal Auditors are acting as an agent of the University and as such any investigation, undertaken by them, will substitute for the preliminary investigation outlined in paragraphs 1.7 and 1.8 of the University's Disciplinary Procedures.

(vii) Fraud and Theft Response Team

If required, and as soon as practicable (ideally within 24 hours) a meeting of the Fraud and Theft Response Team should be convened, normally consisting of the following group, to decide on the path of action.

- Chief Strategy & Finance Officer (Chair)
- Chief People Officer (Deputy Chair)
- Director of Risk & Resilience
- Director of Finance
- Director of People and Culture (Partnerships and Services).
- Other co-opted individuals as deemed necessary

It may also be necessary to involve colleagues in communications if there are potential public relations and/or media issues.

This group will:

- Implement the University's [Fraud and Theft Response Procedure](#) (which accompanies this policy)
- Consider the information available (via the Fraud Notification Form if one has been submitted).
- Decide:
 - Whether an investigation is required.
 - If so, commission the investigation, determine who should undertake it, and the composition of any project group set up to co-ordinate it. (Where this relates to a member

- of staff, the investigation will be conducted in line with the provisions of the staff Disciplinary Procedures).
- Whether, and at what stage, Internal Audit need to be involved in the investigation.
- Whether the University's insurers need to be informed.
- Whether the staff member(s) or student(s) need to be suspended.
- Consider the corporate reporting responsibilities including:
 - Whether the matter should be reported to the police.
 - What stakeholder communications should be undertaken at this stage e.g. including notifying the Vice Chancellor, Internal and External Auditors, Chairs of Council and ARC, and DfE, as outlined in the Financial Memorandum.

Where the investigation relates to a member of staff, it will be conducted in line with the provisions of Part One of the University's Disciplinary Procedures. The University may ask external experts (e.g. the University's Auditors) to support the investigation. The staff member has the right to be accompanied by a colleague or Trade Union representative to any interviews.

(viii) Director of Risk & Resilience

The Director of Risk & Resilience will act as the University's Fraud Control Officer responsible for coordinating and implementing the University's fraud risk management Framework.

Additional responsibilities will include:

- Convening the Fraud and Theft Response Team upon receipt of a fraud notification and briefing members of findings.
- Acting as the lead liaison with the Internal Auditors if acting as an agent for the University in any investigation.
- Supporting the chair of the Fraud and Theft Response Team by:
 - Drafting and circulating Fraud Notification Forms to relevant stakeholders
 - Drafting and circulating correspondence to staff and students who have allegedly committed fraud.
- Developing training and awareness activities to promote understanding and compliance with the Fraud Risk Management Policy.
- Coordinating the annual review of management's fraud risk assessment for consideration by RMC and maintain the fraud risk register.
- Developing, disseminating and analyzing fraud awareness surveys to continually improve the University's internal controls against fraud.
- Maintaining a Fraud Register for quarterly reporting to the Audit and Risk Committee.
- Compiling the annual Fraud Report for consideration by Audit and Risk Committee.

(ix) Employees

Strong controls against fraud are the responsibility of everyone in the organization. All levels of staff within the University will:

- Complete the [Fraud Awareness training module](#) on the University's Learning Management System.
- Have a basic understanding of fraud, be aware of red flags, be familiar with the types of fraud that might occur within their areas of responsibility and be alert to any indications of fraud.
- Understand their roles within the internal control framework. Employees must understand how their job procedures are designed to manage fraud risks and when noncompliance may create an opportunity for fraud to occur or go undetected.
- As required, participate in the process of creating a strong control environment and designing and implementing fraud control activities, as well as participate in monitoring activities.
- Read, understand and affirm University policies (Section 3) and procedures designed to mitigate fraud and theft.
- Report concerns, suspicions, or incidences of fraud; and cooperate in investigations.

B. Fraud Risk Management Framework

The University's Fraud Risk Management Framework is administered by the Director of Risk & Resilience who reports to the Audit and Risk Committee on matters involving fraud risk. The Framework reflects the concepts of governance, risk assessment, fraud prevention and detection, investigations and corrective action, and monitoring.

Each component of the Framework is designed to help mitigate potential fraud and theft identified during management's fraud risk assessment. Each component is documented within this Policy and periodically updated to reflect the evolving nature of fraud risk within the University's operations.

C. Fraud Risk Assessment

The University is committed to the timely prevention and detection of fraud and theft and is mindful of the UK Government's Failure to prevent Fraud Offence¹. The RMC, with help from Internal Audit, conducts an annual fraud risk assessment to identify, assess, and respond to key fraud risks in the University. Evidence of this self-assessment must be recorded in a fraud risk register with a description of the risk and associated control(s) mitigating the risk identified.

The fraud risk assessment process considers key factors that drive fraud such as opportunities, incentives and pressures, and attitudes and rationalisation. The risk assessment methodology consists of:

- identifying business unit and process-level fraud risks using common fraud scenarios;
- prioritising the likelihood and impact of such risks on an inherent and residual basis through review by the Risk Management Committee;
- mapping fraud risks to internal controls;
- and identifying potential gaps or enhancement opportunities related to management's anti-fraud control activities.

The results of management's fraud risk assessment are addressed within an action plan and shared with the Audit and Risk Committee.

D. Fraud Prevention and Detection Controls

The University has designed a combination of preventive and detective anti-fraud control activities which occur at various levels of the University and are intended to help mitigate the occurrence of fraud and theft as well as ensure the timely detection of fraud risk events within operations.

The University's high-level fraud prevention control activities include:

- Human resource procedures such as selected pre-employee background checks, training, employee surveys, and exit interviews.
- Physical access control activities address admittance to the University's facilities and right to use of assets, such as inventory.
- Logical access control activities address access rights to sensitive information.
- Transaction control activities address procurement procedures and managerial approval requirements.
- Separation of duties to ensure that key functions and controls are not performed by the same person.
- Adequate supervision and workload management.
- Technological control activities include electronic third-party screening activities and automated restrictions on certain payments that present elevated risk to the University or do not comply with prescribed University policy requirements.

The University's high-level fraud detection control activities include:

¹ Under the new offence, an organisation will be liable where a specified fraud offence is committed by an employee or agent, for the organisation's benefit, and the organisation did not have reasonable fraud prevention procedures in place.

- Data analytics utilised by the Finance directorate to continuously monitor certain types of payments and transactions, as well as data analytics used by the internal audit function in its performance of operational audits (as relevant).
- Reporting mechanisms to receive, retain, and treat concerns, complaints, and information about potential violations of fraud across the University's operations.
- Line management review and approval of staff activity including but not limited to spend requests, reports, etc.
- Periodic reconciliations of accounts.
- Rotation of staff.
- Random spot checks.
- Complete and secure audit trails.
- Appropriate performance monitoring.
- Frequent budgetary and other financial reviews/reports.
- Periodic reviews by independent bodies such as Internal Audit.

5. Fraud Reporting

All attempted, suspected or actual incidents should be reported immediately either:

- To the Head of Department and/or the Chief Strategy & Finance Officer. The Head of Department should then inform the Chief Strategy & Finance Officer or, in their absence, the Chief People Officer.
- Anonymously via the [Reporting a Fraud](#) form.
- Via the University's [Raising Concerns \(Whistleblowing\) Policy](#); provided reports are made in good faith then an individual is protected by the University against harassment or victimisation and the individual's confidentiality must be preserved. The University Secretary, on receiving notifications allegedly related to fraud, will inform the Chair of the Fraud and Theft Response Team. The Team will determine if the matter should progress through the Fraud and Theft Response route or the Whistleblowing route.
- By sending an email to fraud@ulster.ac.uk

If the disclosure involves or implicates any of the individuals identified above, then the disclosure should be made to the Vice Chancellor and/or the Chair of University Council and/or the Chair of Audit & Risk Committee as appropriate. If the disclosure relates to the Vice Chancellor, the matter should be raised with the Chair of Audit and Risk Committee. Contact details for the Chairs of Council and Audit and Risk Committee can be obtained from the University Secretary.

On being alerted to circumstances which give rise to suspicion of fraud or theft, the Director of Risk & Resilience, under the instruction of the Chief Strategy & Finance Officer will convene a meeting of the Fraud and Theft Response Team (and Head of Department if deemed necessary) who will then review the preliminary findings and, where appropriate, in conjunction with the Chief People Officer decide whether to:

- Discontinue the investigation if initial suspicions are not confirmed, or
- Continue with a full internal investigation.
- Engage the assistance of Internal Audit.

Third parties are encouraged to report fraud impacting the University either through the [Raising Concerns \(Whistleblowing\) Policy](#) or by sending an email to fraud@ulster.ac.uk

6. Fraud Response Procedures

The University's [Fraud and Theft Response Procedure](#) outlines the process to be adopted if attempted, suspected or actual fraud is reported or detected and clearly defines the authority levels, responsibilities for action and reporting lines.

7. Monitoring of Fraud Policy Effectiveness

The design of the components within the fraud risk management framework will be evaluated during management's annual fraud risk assessment, or sooner, should a fraud risk event occur. The operating effectiveness of related anti-fraud controls will be tested periodically by Internal Audit.

Periodically, the internal audit function may conduct a separate and independent evaluation of the fraud risk management framework utilising authoritative guidance and leading practices. Internal audit will report its findings to the Audit and Risk Committee and management. The fraud control officer is responsible for ensuring that any deficiencies, weaknesses, or enhancements involving anti-fraud controls are addressed in a timely and effective manner. In addition, internal audit will consider the risk of fraud as part of its operational audits conducted throughout the course of the year.

8. Training

[Training on Fraud Awareness](#) should be completed by all staff on the Learning Management System and refreshed every two years.

Targeted technical training should be provided on the fraud risk management process e.g., training on conducting risk identification, assessment and the codification of risk and control on the fraud risk register. Senior Managers are responsible for ensuring that the right staff members are identified to attend the training session.

9. Policy Non-Compliance

If non-compliance with this policy is identified, the policy owner and/or the Fraud and Theft Response Team must assess the impact of the non-compliance and document, as appropriate, the planned remediation. Any instances of policy non-compliance must be logged on the fraud risk register with a corresponding action plan detailing the planned remediation.

10. Policy Review

This Policy will be assessed by management and reviewed by the University's Audit and Risk Committee every three years. Any changes to the Policy will be communicated to University staff and relevant third parties in a timely manner.

Appendix 1 – Sample Definitions

Fraud:

- Wrongful or criminal deception intended to result in financial or personal gain
- A person or thing intended to deceive others, typically by unjustifiably claiming or being credited with accomplishments or qualities
- A false representation of a matter of fact - whether by words or by conduct, by false or misleading allegations or by concealment of what should have been disclosed
- A deception practiced in order to induce another to give up possession of property or surrender a right

Corruption:

- The use of public office for private gain
- Dishonest or fraudulent conduct by those in power, typically involving bribery

Bribery:

- The offering, giving, receiving, or soliciting of something of value for the purpose of influencing the action of an official in the discharge of his or her duties
- Money, favour or benefit given or promised in order to influence the judgment or conduct of a person in a position of trust

Theft:

- The illegal taking of someone else's property without that person's freely-given consent. Apart from the obvious theft of physical assets such as computers, stock and money, it includes:
 - Misappropriation of funds
 - Misuse of assets, including cash, stock and other assets, for example 'borrowing' petty cash,
 - Theft from a client or supplier
 - Theft of intellectual property, including designs and data

Misuse of resources:

- The use of photocopiers for private purposes.

Deception:

- To intentionally distort the truth in order to mislead others. It would include obtaining property, services or pecuniary advantage by deception or evading liability. Deceptions typically include:
 - Misrepresentation of qualifications to obtain employment
 - Obtaining services dishonestly via technology
 - Undeclared and unauthorised private and consultative work

Forgery:

- Making or adapting objects or documents with the desire to deceive

Extortion:

- Obtaining money or property from another through coercion or intimidation

Embezzlement

- Fraudulent appropriation by a person to their own use of property or money entrusted to that person's care but owned by someone else

Conspiracy:

- An agreement between two or more persons to break the law at some time in the future

Collusion:

- Any case in which someone incites, instigates, aids and abets, conspires or attempts to commit any of the crimes of fraud

Money Laundering:

- How criminals process illegal or dirty money derived from the proceeds of any illegal activity through a succession of transactions and deals until the original source of such funds has been obscured and the money take on an appearance of legitimate or clean funds - involves placement, layering and integration of the money

Appendix 2 – Indicators and Warning signs of fraud

Fraud Indicators can include:

- Staff exhibiting unusual behaviour (see list above)
- Missing key documents, especially invoices and/or contracts
- Inadequate or no separation of duties
- Documentation which is photocopied or missing key information
- Missing expenditure vouchers
- Excessive variations to budgets and/or contracts
- Bank and ledger reconciliations not regularly preformed and cannot be balanced
- Numerous adjustments or exceptions
- Overdue pay or expense advances
- Duplicate payments
- Ghost employees on payroll
- Large payments to individuals
- Lack of bank account controls
- Crisis management coupled with a pressured work environment
- Lowest tenders or quotes passed over without adequate explanation
- Single vendors
- Climate of fear/low staff morale
- Consistent failure to implement key controls
- Controls frequently overridden

Warning signs can include:

- Staff under stress without a high workload
- Reluctance to take annual leave
- Being first to arrive in the morning and last to leave in the evening
- Refusal of promotion
- Unexplained wealth
- Sudden change of lifestyle
- Suppliers/ contractors who insist on only dealing with one staff member
- Individuals seen as risk-takers or rule-breakers
- Disgruntled at work and/or not supportive of the University

Appendix 3 – Examples of controls to prevent and detect fraud

- Comprehensive recruitment procedures, with full reference checks
- Physical security of assets
- Adequate supervision and workload management
- Separation of duties to ensure that key functions and controls are not performed by the same person
- Rotation of staff
- Random spot checks
- Complete and secure audit trails
- Appropriate performance monitoring
- Frequent budgetary and other financial reviews/reports
- Periodic reviews by independent bodies such as Internal Audit