University of Strathclyde Glasgow

Counter Fraud Policy

Policy Owner	Date of latest review	Approval	Effective Date	Next Review Date
University Compliance Officer	May 2023	Executive Team/ Audit & Risk Committee/ Staff Committee	October 2023	
University Compliance Officer	May 2026	Executive Team/ Audit & Risk Committee/ Staff Committee/Court	10th June 2026	June 2028

Counter Fraud Policy
Contents

1. INTRODUCTION 3
2. DEFINITION AND EXAMPLES OF FRAUD AND SUSPICIOUS ACTIVITY 4
3. SCOPE 4
4. STRATEGIC APPROACH 5
5. PREVENTION 6
6. DETECTION 8
7. STAFF RESPONSIBILITIES 9
APPENDIX 1 – FRAUD RESPONSE PLAN 12
1. INTRODUCTION AND FRAUD RESPONSE GROUP 12
2. INITIATING ACTION 12
3. PRELIMINARY FACT-FIND INVESTIGATION 13
4. SUBSTANTIVE INVESTIGATIONS 15
5. CONCLUDING AN INVESTIGATION 16
6. REPORTING RESPONSIBILITIES 17
7. RECOVERY OF LOSSES 18
8. EXTERNAL FRAUDS 18
9. REVIEW OF THE FRAUD RESPONSE PLAN 19
APPENDIX 2 – EXAMPLES OF FRAUD, SUSPICIOUS ACTIVITY AND BEHAVIOURAL INDICATORS 20
APPENDIX 3 – WHAT TO DO AND NOT DO IF YOU SUSPECT FRAUD 23
APPENDIX 4 – FRAUD INVESTIGATION CHECKLISTS 24
APPENDIX 5 – FRAUD REPORTING FLOWCHART 26
APPENDIX 6 – FURTHER REFERENCE 27
APPENDIX 7 – FRAUD RISK MANAGEMENT FRAMEWORK 28
APPENDIX 8 – CORE ROLES AND RESPONSIBILITIES OF FRAUD RESPONSE GROUP 29
APPENDIX 9 – PROTOCOL FOR UNDERTAKING INVESTIGATIONS UNDER THE FRAUD POLICY 31

1. INTRODUCTION

1.1. The University's activities require significant funds, some of which are 'public'. As a publicly funded body, the University is accountable to a wide range of stakeholders for the use and management of those funds, and the associated controls.

The University also administers or jointly administers other funds and financial schemes, including for example Research Council funding, Student Loans Company funding and Student Awards Agency Scotland support. This Policy applies equally to those arrangements and to the conduct of the University, its staff and its students where they are acting in connection with, accessing, administering, certifying, claiming, receiving or otherwise participating in such funding or support arrangements.

The University is committed to the highest standards of openness, probity and accountability. It will not tolerate fraud and is committed to reducing its risk of fraud to the lowest possible level. This Counter Fraud Policy (the "Policy") is a public statement of the University's top-level commitment to prevent, detect and act upon cases of fraud and suspicious activity in a robust manner. The purpose of the Policy is to further enhance systems, policies and procedures which deter acts of fraud and to encourage development of an anti-fraud culture. The Fraud Response Plan, set out in Appendix 1 of the Policy, sets out the steps to be followed in the event that a suspected fraud is uncovered.

1.2. This Policy aims to emphasise the responsibilities of all staff and students in relation to the identification and reporting of fraud and suspicious activity, including cyber fraud. A counter fraud culture, aligned with good awareness of both internal controls and the possible indicators of fraud will help to ensure that the University continues to protect its assets and safeguards its receipt and disbursement of public monies.

1.3. The University Compliance Officer (UCO) is the Designated Person with responsibility under the Policy. The Chief People Officer shall deputise as the Designated Person in the absence of the UCO, whom failing, the Chief Financial Officer. The University's commitment to a counter fraud culture is regularly communicated from the Executive Team which firmly rejects **fraud** in all its forms and will not tolerate it either within our business, or within the operations of our business partners that provide services for us or on our behalf. Our mission is to **prevent fraud** by fostering a culture of honesty and accountability.

1.4. On 1st September 2025 a new "failure to prevent fraud" offence (the **FTPF Offence**) was introduced as part of the Economic Crime and Corporate Transparency Act (**ECCTA**). Under ECCTA, large organisations, including the University, will be criminally liable if an Associated Person[1] commits one of the specified **fraud** offences

[1] An Associated Person can be an employee, agent, subsidiary undertaking or employee of a subsidiary undertaking of the University and/or those who otherwise perform services for or on behalf of the University ("Associated Person"). In the University context, an Associated Person may include for example members of staff (including visiting academics delivering lectures on behalf of the University), subsidiaries and commercialisation vehicles of the University in the UK and overseas (including their staff), transnational education partners, delivery partners, overseas recruitment agents, property management agents, payment collection agents, marketing agencies, IP licensing agents, research partners, consultants and any other suppliers who are acting as representatives or otherwise on the University's behalf.

(including common law fraud and embezzlement in Scotland) with the intention of benefitting either the organisation or any person to whom the organisation or its subsidiary provides services. The only defence to the FTPF Offence is that the University had reasonable procedures in place to **prevent** the relevant **fraud.** The FTPF Offence places a significant responsibility on the University to establish and maintain a robust fraud risk management framework. Non-compliance can result in severe penalties, including fines. The FTPF Offence does not apply where the University was, or was intended to be, the victim of the underlying fraud.

2. DEFINITION AND EXAMPLES OF FRAUD AND SUSPICIOUS ACTIVITY

2.1. DEFINITION

In the context of this Policy, the term Fraud means the use of deception to bring about a practical result which could include a gain or avoidance of an obligation that causes loss to another person or organisation. Fraud may not always be immediately apparent. Accordingly, this Policy also refers to *suspicious activity*, which includes indicators or behaviours that could suggest Fraud or attempted fraud. Employees and others working on behalf of the organisation are not expected to determine whether fraud has occurred but are expected to report suspicious activity promptly so that it can be reviewed and, where appropriate, investigated.

Fraud is taken to include, but not limited to, theft (physical and cyber), misuse of property, corruption, the alteration of financial or other records, deception, bribery, extortion, conspiracy, embezzlement, false representation or misstatement, concealment of material facts and collusion.

Generally, the intention to deceive is the crucial component of Fraud. However, certain types of fraud can occur where there has been, for example, reckless or negligent disregard for the truth rather than intentional deception. All types of Fraud fall within the scope of this Policy.

The intended practical result can relate to the University itself, as well as an individual or an Associated Person, e.g. a supplier of the University. The intended practical result does not have to be financial, for example an employee could benefit from omitting perceived laborious administration or be coerced into circumventing University guidance, with no personal gain. The deception may result in a gain, as well as a loss to another party, for example, a supplier may have additional activity added into a contract.

2.2. EXAMPLES

Examples of Fraud and suspicious activity can be found at Appendix 2 of this Policy.

3. SCOPE

3.1. This Policy is applicable to all staff, students and applicants of the University, agents, suppliers, research partners, other volunteers/lay members and Associated Persons (as earlier defined). Any fraudulent activities identified in relation to other individuals working with, or on behalf of, or for the University should be reported through the relevant processes noted in this Policy. Where a suspected Fraud is associated with activities

undertaken through University of Strathclyde Students' Association (USSA), the University will work with USSA in line with relevant USSA and University policies.

3.2. The University takes any allegations of Fraud seriously and will investigate all such concerns. Staff members or students found to be committing fraud (attempted or actual) may be subject to disciplinary proceedings which may result in dismissal or expulsion. The matter may also be referred to the police and other appropriate organisations, e.g. Information Commissioner, Student Awards Agency Scotland, National Crime Agency for instances of money laundering. The ECCTA legislation notes the term 'agent' is governed by domestic law and typically includes anyone with authority to enter into contracts on behalf of the entity. Any suspected Fraud relating to an Associated Person would be investigated under the provisions of this Policy and may result in termination of contracted services.

4. STRATEGIC APPROACH

4.1. The University has a zero-tolerance policy towards Fraud whether that is actual or attempted. The University Court and its Executive Team is committed to preventing Fraud and fostering a culture in which deception is never acceptable. The University recognises the long-term benefits of rejecting fraudulent practices, including enhanced reputation, increased customer confidence and sustainable business growth The University has a strong commitment to preventing and detecting fraudulent behaviour. If Fraud is suspected it will be investigated professionally and thoroughly. Processes and procedures will be reviewed and monitored to ensure they are effective and efficient.

4.2. The key objectives of this Policy are:

- Prevent instances of Fraud from occurring in the first place;
- Detect instances of Fraud when they do occur;
- Respond appropriately and take corrective action when instances of Fraud arise;
- 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 fraud has been perpetrated.

4.3. The University has a Fraud Risk Management Framework, a summary of which is contained in Appendix 7. The Framework sets out at a high level the governance arrangements the University has in place to prevent, detect, report and investigate fraud. The University undertakes periodic fraud risk assessments, in respect of current and emerging risks and both "benefit-to-institution" and "fraud-against-institution" scenarios. Line managers should ensure that local risk registers are maintained up to date, including considering fraud risks where appropriate, for example cyber-enabled fraud, overseas partnerships, research funding fraud, changes to systems or processes or new partnerships/ventures.

4.4. The Counter Fraud Group (CFG) is chaired by the University Compliance Officer and provides governance over the Fraud Risk Management Framework and strategic direction to the University on counter-fraud activities. The CFG plays a central role in reviewing University processes for the prevention, detection and management of Fraud risks, and promotes a fraud awareness culture of integrity, and zero tolerance of Fraud, bribery and related misconduct across the University. CFG reports annually to Executive Team and Audit & Risk Committee.

4.5. The Fraud Response Group is chaired by the University Compliance Officer and oversees the investigation of any reported Fraud. Its remit and purpose is described in more detail in Appendix 8 of this Policy.

5. PREVENTION

5.1. The aftermath of Fraud is costly, time-consuming and disruptive, and may lead to unwelcome adverse publicity. Staff and students should contribute to a work and study environment in which fraudulent activity is actively prevented through a number of means.

Leadership

5.2. The tone from the top is critical in influencing behaviour within the University. Chief Officers, Executive Deans and senior managers should therefore ensure that their behaviour always adheres to the highest principles of integrity. An open and transparent culture is critical, where staff and students feel able to challenge unusual activity and raise concerns without fear of reprisal.

Relevant Policies and Procedures

5.3. The University seeks to minimise the opportunities for Fraud through carefully designed and consistently operated management procedures. Day to day responsibility for the prevention and detection of fraud rests with line managers who are responsible for the implementation of policies and procedures for operations within their area of responsibility. These should be regularly risk assessed and reviewed to ensure they remain robust, up-to-date and fit for purpose. Should staff become aware of any weaknesses in controls within their areas, they should alert line management (or line manager's manager if line manager believed to be involved) of this immediately.

5.4. The University may elect to use more than one procedure, or a hybrid of procedures depending on the circumstance, where appropriate having consideration of the Fraud Response Plan in Appendix 1; for example, and without limitation, in respect of Fraud, the Staff Disciplinary Procedure may be utilised in conjunction with the protocol defined within the Fraud Response Plan in Appendix 1. Suspected fraudulent acts undertaken by a student may be referred for action under the University's Student Discipline Procedure in conjunction with the Fraud Response Plan in Appendix 1. Fraud or Suspicious Activity may be reported via a complaint under the Complaints Handling Process. Any such case should be initially escalated to the Designated Officer in line with Clause 7.11 for consideration as to which process should be initiated to investigate the matter.

5.5. The University publishes and widely disseminates a range of approved regulations, policies and procedures which contain measures aimed at preventing Fraud; please refer to Appendix 6 Further Reference section. A number of these policies are inter-dependent with regards to Fraud and any investigations initiated under the Fraud Response Plan must be mindful of this and work within the framework of such policies, where relevant. Declarations of Conflicts of Interest and Receipts of Gifts and Hospitality should be maintained locally, in line with relevant University Policies.

Due Diligence

5.6. The University recognises that effective due diligence is a key preventative measure in reducing the risk of fraud, financial crime, reputational damage and regulatory non-compliance. Staff should apply risk based, proportionate due diligence to individuals

and organisations with whom they engage, including third parties, partners and donors. Where appropriate, concerns will be escalated for enhanced review.

Due diligence requirements may vary proportionate to the value and risk of the activity, but will typically include the following elements:

- appropriate pre appointment and ongoing checks to ensure that individuals engaged by the University are suitable for their role and meet required standards of integrity and competence;
- due diligence on suppliers, agents, contractors, collaborators, partners, and Associated Persons to ensure that they are legitimate, financially sound and aligned with the University's ethical and regulatory expectations;
- Pre-acceptance checks that philanthropic donations are accepted in a manner that is lawful, ethical and in accordance with proportionate anti-money laundering requirements e.g. 'know your customer checks'.

Employee Screening

5.7. Potential new members of staff should be screened before appointment particularly for posts with financial responsibility. For example:

- At least two references, one from line manager or HR Department of last employer, should be obtained;
- Doubts about the contents of the reference should be resolved before confirming the appointment. The University will usually require written references but if a telephone reference is obtained, a written record of the discussion should be kept; and
- Essential qualifications should be checked before making an offer of employment such as requiring original certificates prior to commencing employment.

Financial and Operational Controls

5.8. Financial and operational controls should be clearly defined and communicated by line managers. Such controls include:-

(i) segregation of duties in order to prevent one individual from controlling an entire transaction e.g. one person should not be receiving, recording and banking cash;

(ii) Authorisation and approval controls to ensure transactions are legitimate, justified and within delegated authority;

(iii) Budgetary control and monitoring in order to detect anomalies and prevent misuse of funds;

(iv) Payroll and expenses controls such as regular payroll reconciliations, independent review of expenses claims and automated checks for duplicate or out-of-policy claims;

(v) Supplier and Procurement controls such as supplier due diligence and verification; no single officer controlling supplier set up and payment; competitive quotations.

Physical Security

5.9. Managers shall ensure that all cash and assets (including valuable data) are kept and stored securely with clear access rights defined and implemented. Appropriate Asset registers should be completed and kept up to date.

Internal Audit Services

5.10. The University's Internal Audit Service (IAS) is able to offer advice on process design and undertakes internal audit reviews of activity to highlight any areas of vulnerability. Departments or areas with processes more vulnerable to risks associated with fraud should consider seeking the support of IAS to review control mechanisms and propose recommendations for enhancing the control framework.

6. DETECTION

6.1. No framework of preventative measures can guarantee that Frauds will not occur. The key resource for the identification of suspected fraud is the vigilance of staff in their day-to-day work. All employees have a duty under the University's Financial Regulations and other policies listed in Appendix 6 to report suspicion or detection of any incidence of suspicious activity or Fraud at the earliest opportunity. This Section 6 sets out additional detection measures that staff should be aware of and employ as appropriate.

Management Review & Budgetary Monitoring

6.2. There is an expectation that regular budget monitoring and variance analysis is performed, with the investigation of unusual or unexplained movements followed up. Detective checks and balances should be designed into all systems and applied consistently. These should include segregation of duties, reconciliation procedures, random checking of transactions, and review of management information, including exception reports. Management at all levels are responsible for ensuring the effective application of controls.

Financial Reconciliations & Exception Reporting

6.3. Routine, independent reconciliations and the use of exception reports and suspense account reviews identify anomalies that may require further investigation.

Procurement & Partnership Monitoring

6.4. Monitoring of contract performance and payment schedules, as well as periodic review of registers of interests highlight activity out with expectations and may require further escalation. Ongoing due diligence in partnership and donor relationships also can be a detective measure when circumstances change.

Whistleblowing & Complaints Procedures

6.5. The University has a confidential and clearly communicated Whistleblowing Procedure, where instances are recorded and investigated appropriately.

Student payments

6.6. Students and applicants can be victims of Fraud and money laundering because they may be targeted by criminals who exploit their lack of knowledge of the activity. Criminals may use students as "money mules" to move money or to purchase bank accounts and identification details. The University's Anti-Money Laundering Policy

must be initiated where there is any suspicion of money laundering. At no time and under no circumstances should staff or students voice any suspicions to the person(s) suspected of money laundering to avoid the offence of "tipping off" those who may be involved.

Warning signs

6.7. Appendix 2 lists behavioural indicators, which are not exhaustive, which may assist staff in identifying possible signs of Fraud and suspicious activity.

It should be noted that in some cases a student or member of staff may be, knowingly or unwittingly, implicated in a Fraud. Where the student or member of staff has unwittingly or through coercion been implicated in a fraud, this will be considered by the Fraud Response Group in planning and formulating a response to the suspicion.

7. STAFF RESPONSIBILITIES

7.1. All University staff are expected to maintain a high degree of integrity in their decision making and day to day duties. All staff must be aware of the Code of Practice on Conflicts of Interest which also requires certain members of staff to submit an annual declaration of interests and undertake the mandatory training on Conflicts of Interest every 2 years. The University expects its staff to exercise the highest standards of corporate and personal conduct.

7.2. The acceptance of gifts or hospitality is an area of potential corruption in any organisation. The Policy for the Offering or Receipt of Gifts, Hospitality and Other Benefits provides guidance and outlines responsibilities in this area.

7.3. All staff are responsible for:

- Acting with propriety in the use of University resources and in the handling and use of University funds, whether involved with any form of payment systems, receipts or dealing with contractors and suppliers;
- Being alert to the possibility that unusual events or transactions could be indicators of fraud and/or cyber-attacks;
- ensuring that University funds and resources are used honestly and correctly;
- Reporting details immediately in accordance with Sections 7.11-7.14 of this Policy if they suspect that a fraud or irregularity has been committed or see any suspicious acts or events; and
- Co-operating fully with University employees or agents conducting internal checks, reviews and/or fraud investigations.

7.4. Staff are encouraged to bring to management's attention areas of weakness they have identified in the procedures they use and to suggest improvements to these procedures to reduce the possibility of fraud. Confidentiality will be respected where possible.

7.5. Managers should be alert to the possibility that unusual events may be the symptoms of fraud or attempted fraud. Employees with managerial responsibility are also responsible for ensuring that an adequate system of internal control exists within their

area of responsibility, appropriate to the risk involved and that those controls are properly operated and complied with.

7.6. Managers of people have the prime role in the prevention of fraud because the effective enforcement of the University's internal controls fall largely on them. In practice, fraud often occurs because of weaknesses in control – either control processes are absent, ineffective or not being complied with. IAS can provide assistance to managers who require guidance in this area.

7.7. Where there is suspicion that fraud has occurred, or is about to occur, then it is essential that the appropriate person within the University is contacted immediately (see Sections 7.11-7.14). A summary procedural flow chart is included in Appendix 5.

Training

7.8. All staff are expected to be aware of this Policy and the procedures contained within it and are expected to complete the mandatory University Training on Fraud Awareness every 2 years. Role-specific training may be required for higher risk areas e.g. Admissions, International Recruitment, Research Finance, Procurement, Student Finance, Alumni & Development, Commercialisation, Finance Business Partners. In addition, all staff must undertake the mandatory cyber security training and data protection training on an annual basis to ensure they are up to date with current approaches to minimizing fraudulent attempts to acquire University financial resources and personal data.

Reporting of Suspected Fraud

7.9. Suspected fraud can come to light in many ways, including routine checks, concerns raised by staff, students or external parties, and internal or external audit work. The definition of Fraud (Section 2) and the warning signs (Appendix 2) are intended to help identify potential Fraud. Anyone who has a reasonable suspicion of Fraud should report it immediately using the processes below. Reports will be treated in strict confidence. No employee or student will suffer any disadvantage for raising a genuine concern. This protection does not apply where a concern is raised maliciously or is known to be untrue.

7.10. If staff notice something suspicious, they should make a note of any relevant information available without investigating. Appendix 3 of this Policy provides additional guidance around what to do and what not to do if you suspect Fraud or suspicious activity. **Under no circumstances should staff:-**

- Confront the person they suspect
- Carry out their own investigation or gather evidence
- Discuss their concerns with anyone other than through the reporting routes below
- Ignore the concern

7.11. Concerns should normally be reported by emailing fraud-reporting@strath.ac.uk. Alternatively, concerns can be discussed with the relevant Line Manager or, if the Line Manager is involved, the matter should be raised with the next appropriate senior

person. Following discussions, if there are still concerns, these should be reported to fraud-reporting@strath.ac.uk.

For suspected **student fraud**, concerns should be raised with the relevant service area, for example:

- **Student funding or hardship applications** –Deputy Head of Student Advice and Support or Head of Student Advice and Support
- **Admissions** – Faculty Admissions Team, Head of Department and/or Student Experience Admissions Team; for international students, also the Visa Compliance Team and Recruitment & International Office
- **Tuition fees or other payments** – Deputy Director of Finance (Operations)

Students may also use the email address noted above to raise fraud concerns relating to students or staff.

7.12. Where there is a suspected cyber security incident, the IT Helpdesk must be contacted immediately. Where there is suspected loss or theft of personal data, the Data Protection Officer must be contacted immediately.

7.13. If it is not appropriate to use the routes above, concerns may be raised directly with a member of the Fraud Response Group (the UCO, Chief People Officer, Chief Financial Officer, Head of Legal Services and/or the Head of Internal Audit) or the Convener of the Audit & Risk Committee.

7.14. If staff feel unable to follow these fraud reporting processes, then they can use the University's **Public Interest Disclosure (Whistleblowing) Policy and Procedures**.

Senior Officers, Executive Deans, Heads of Department/Schools, Directors Line Managers and any staff member receiving a fraud report must be aware that suspected individuals have rights under University policy. No action, including interviewing staff, should be taken without prior consultation with the University Compliance Officer. **Appendix 4** provides a checklist for managers following the reporting of suspected fraud.

APPENDIX 1 – FRAUD RESPONSE PLAN

This document should be read in conjunction with the University's Counter Fraud Policy.

1. INTRODUCTION AND FRAUD RESPONSE GROUP

1.1. The purpose of this Fraud Response Plan (the "Plan") is to outline the steps to be followed in the event that a suspected Fraud is uncovered. This Plan provides a consistent framework for investigating and reporting Fraud and considers where there are associated risks in connection with breaches of cyber security and breaches of data protection legislation.

1.2. The Fraud Response Group (FRG) consists of the Designated Person (University Compliance Officer and Convener), Chief People Officer, Chief Financial Officer, the Head of Legal Services, in an advisory capacity, and the Head of Internal Audit. The FRG is the University's designated cross-functional team that responds to reports of suspected or actual Fraud and coordinates how fraud is investigated, managed, and resolved. The core responsibilities of the FRG are set out in Appendix 8. The Chief People Officer shall deputise as the Designated Person in the absence of the UCO, whom failing, the Chief Financial Officer.

1.3. If any suspected Fraud directly involves a member of the FRG or a member of their teams or a matter in their area, then that member will recuse themselves from the activities of the FRG and may be replaced by a Senior Officer nominated by the Principal if the remaining members of the FRG believe this is appropriate.

1.4. Depending on the type of suspected Fraud, and only where necessary, the Designated Person may invite additional members of staff with specialist expertise to join the FRG, for example, the Cybersecurity Manager in the event of suspected cyber fraud or the Data Protection Officer in the event of suspected theft of personal data.

1.5. In the absence of any member of the Fraud Response Group specified, a nominated depute shall attend.

1.6. The University shall maintain a centralised Suspicious Activity Log for recording both suspected and confirmed incidents of Fraud. The Suspicious Activity Log will include reference to any associated investigations and outcomes and will be kept for six years and where any investigation has resulted in termination of employment the records shall be kept for 6 years post termination. The designated person shall be responsible for maintaining the Suspicious Activity Log and ensure that all members of the FRG have access to this.

2. INITIATING ACTION

2.1. All cases of suspected or known Fraud should be reported immediately through the appropriate reporting route noted in Sections 7.11-7.14 of the Policy and, regardless of the apparent amounts involved, to the University Compliance Officer (the Designated Person). Where required, the Designated Person should convene a meeting of the University's FRG as soon as possible. A dedicated minute taker will support the work of the FRG and ensure all actions are recorded via an action tracker. There will be

systematic documenting of meetings, decisions, communications and actions. All such documentation will be made available to members of the FRG in a secure manner.

2.2. In the case of suspected student Fraud, the University Compliance Officer will consult with the Director of Student Experience, Deputy Director of Finance and/or Head of Internal Audit and such other relevant members of staff (as appropriate) to determine whether the FRG should be convened or the case should be dealt with under the appropriate procedure, e.g., the Student Discipline Procedure, the Admissions Policy.

2.3. Following the reporting of an alleged Fraud under this Policy, the FRG should consider and, where appropriate, address all of the points set out in the Checklist at Appendix 4. Prior to initiating any investigation under this Policy or any other relevant University policy, the FRG should consider and decide, based on all of the information available to it, which policy is relevant to the Fraud in question and should therefore be invoked.

It may be that a preliminary fact find investigation and/or substantive investigation under this Plan needs to be undertaken before such a decision can be made. The FRG should ensure that in deciding the route for investigation that it clearly articulates and documents:-

1. The decision-making process regarding policy selection;
2. Investigation routes;
3. interested parties;
4. employee information sharing i.e. at what stage the suspected individuals or their line managers can be involved in an interview; and
5. reporting lines.

2.4. To avoid layers of complexity, the FRG should instruct all preliminary fact-find and substantive investigations relating to a Fraud. No additional or simultaneous investigations should be carried out. The primary fraud investigation should take priority to be as effective and efficient as possible, as well as to avoid 'tipping off' and safeguarding evidence. All staff should cooperate fully and respond expediently to the appointed Investigating Officers' information requests.

2.5. The FRG must uphold and emphasise to the Investigating Officer the independence of any investigations under this Plan and acknowledge that, under no circumstances, any undue influence should be exerted on Investigating Officer to alter their investigative findings or recommendations. Any instances of attempts to interfere with a fraud investigation should be logged on the Suspicious Activity Log in the Fraud Investigation file. This includes intimation of the interference to the FRG, any emails, notes of conversations, etc.

2.6. The Designated Person should advise the Principal and Convener of Audit & Risk Committee, at the earliest stage, when an investigation has been initiated.

3. PRELIMINARY FACT-FIND INVESTIGATION

3.1. After consultation with the FRG and where it has agreed to be appropriate having considered all of the available facts, the Designated Person may appoint an Investigating Officer to undertake a preliminary fact-finding investigation. This is to seek background information, identify further sources of evidence, obtain a quick understanding of the matter and provide context to an allegation before the remit and scope of any substantive investigation has taken place. Any preliminary fact-finding

investigation must be conducted in accordance with the Protocol for Undertaking Investigations under the Fraud Policy set out at Appendix 9 and in a manner which is both rigorous and timely and maintains strict confidentiality subject to the need to share information with appropriate members of staff or external organisations e.g. the Police, Scottish Funding Council, National Crime Agency, External Auditors.

3.2. The FRG shall continually review progress being made on the fact-finding investigation, to verify that the Investigating Officer is receiving the support and information they require and to ensure that the investigation concludes as soon as possible.

3.3. The Investigating Officer should produce a preliminary fact-finding report, for consideration by the Fraud Response Group, which will provide sufficient detail to allow an assessment to be made as to whether a Fraud has occurred. The preliminary report should:

- set out the findings to date;
- set out the interim conclusions drawn from those findings;
- set an action plan to continue the investigation, if this is considered appropriate.

The FRG should agree whether the preliminary fact-finding report provides reasonable grounds for suspecting an employee(s) or student(s) or third party of the University of Fraud and whether:-

- a substantive investigation is required under Section 4 of the Plan;
- the matter can be directly referred to the appropriate University Policy for disposal e.g. Staff Discipline Policy; Student Non-academic Discipline Procedure; or
- the matter can be directly referred to the appropriate University Policy prior to any substantive investigation.

3.4. Following the submission of the preliminary fact finding report, the Suspicious Activity Log will be updated accordingly.

SUSPENSION

3.5. Where the preliminary fact-find investigation provides reasonable grounds for suspecting an employee(s) or student(s) or third party of the University of Fraud, a decision should be taken as to whether the suspected employee(s)/student(s) should be suspended. The Chief People Officer or University Secretary or their nominees (as appropriate) should progress any suspension and/or restricted access in accordance with normal agreed disciplinary procedures, however, it may be necessary to plan the timing of any suspension to prevent the suspected employee(s) or student(s) from destroying or removing evidence that may be needed to support disciplinary or legal action.

3.6. In these circumstances the employee or student should be approached unannounced. They should be supervised at all times before leaving the University's premises. They should be allowed to collect personal property, under supervision, but should not be able to remove any property belonging to the University. Any security passes, laptops and mobile devices, keys to premises, offices and furniture should be returned.

3.7. The Deputy Director of Estates / Head of Security Services (or nominee) or appropriate University employee should advise on the best means of denying access to the University whilst the employee/student remains suspended. The Director of Information Services (or nominee) should be instructed to withdraw, without delay, access permissions to the University's computer systems. The requirement for suspension will be reviewed regularly throughout the investigation and any subsequent disciplinary action.

3.8. If an employee/student is not suspended, this aspect should be kept under review by the FRG at all stages of the ensuing investigation.

4. SUBSTANTIVE INVESTIGATIONS

4.1. Where the preliminary fact-find investigation provides reasonable grounds for suspecting an employee(s) or student(s) or third party of the University of fraud, a decision should be taken by the FRG as to the nature of any required substantive investigation. The substantive investigation will take place under the policy deemed most appropriate to the investigation, as decided by the Fraud Response Group. The FRG should agree and set the remit, scope and reporting expectation and timeline of any such investigation with input from the area under which the policy sits, as appropriate. The FRG will decide on whether the investigator under the preliminary fact-find investigation should undertake any subsequent investigation or whether a suitable alternative investigator should be appointed under a separate policy, as appropriate. The FRG may seek advice and input from the relevant area in this regard. Any substantive investigation must be conducted in accordance with the Protocol for Undertaking Investigations under the Fraud Policy set out at Appendix 9. A substantive investigation might also form the basis of a staff disciplinary process or student discipline procedure. In such instances, advice should be taken from HR and/or Education Enhancement (Senate Office), as appropriate.

4.2. The Investigating Officer shall consider whether other systems or processes should be reviewed as deemed relevant, where these may have provided additional opportunities for the employee or student to commit fraud. Any related concerns will be reported to the FRG within the final report.

4.3. The FRG shall continually review progress being made on the investigation, to verify that the Investigating Officer is receiving the support and information they require and to ensure that the investigation will conclude as soon as possible.

4.4. At the conclusion of the substantive investigation a final report will be produced by the Investigating Officer appointed under Clause 3.1. This report will be submitted to the Fraud Response Group and the Designated Person will inform the Principal and the Convener of the Audit & Risk Committee of the findings.

4.5. If the circumstances set out in the final report indicate that an employee/student has a case to answer, the Designated Person, under the direction of the FRG, will invoke the University’s internal disciplinary procedures if not already invoked.

4.6. Following the submission of the final report, the Suspicious Activity Log will be updated accordingly.

5. CONCLUDING AN INVESTIGATION

DECISION MAKING

5.1. At the conclusion of the substantive investigation the FRG will review the final report produced by the Investigating Officer and, where appropriate, will be appraised of its conclusions, how recommendations have been communicated to the recipients, and how these actions will be tracked to completion. Dependent on the route of investigation, this may or may not be designated to the FRG. In all cases, the FRG shall ensure an appropriate decision has been reached on disposal of each Fraud case and that all appropriate individuals have been informed of the outcome of the investigation.

5.2. Following review of the final report, the FRG will:-

I. acknowledge to the fraud investigators that FRG has reviewed the fraud investigation report;
II. document the decisions made based on the fraud investigation report review;
III. document how the FRG has advised relevant managers of any further remedial / disciplinary action required if this has not already occurred; and
IV. document how any required actions are followed up to verify their completion.

This record of events should be updated in the Suspicious Activity Log by the FRG.

5.3. IAS will monitor the implementation of any recommendations / actions agreed in response to a Fraud investigation in parallel with the reporting to the Audit & Risk Committee of management actions arising from Internal Audit reviews.

5.4. On completion of an investigation, a written report should be submitted to the Audit & Risk Committee for consideration and discussion. This report will normally be prepared by the Fraud Response Group and will include:

- A description of the incident, including the value of any gain or loss, the people involved, and the means of perpetrating the fraud;
- Actions taken to prevent a recurrence;
- A plan detailing any recommendations and actions (with action owners and implementation timelines identified) required to strengthen future fraud responses.

LESSONS LEARNED

5.5. At the end of a Fraud investigation, irrespective of the outcome, it is important that the progress of the investigation is reviewed to see what lessons can be learned, to identify improvements and to assess the effectiveness of the action taken. Such reviews will help identify any weaknesses in internal control that initially led to the Fraud and should highlight any deficiencies in these systems for reporting and investigating, enable more effective future enquiries and precipitate changes to internal procedures designed to prevent recurrence. Reviews should be undertaken

following the conclusion of every Fraud investigation by the FRG and should involve interviewing the Investigating Officer.

Lessons learned will be used to refine policies and procedures as well as enhancing awareness of fraud risks among staff and students.

6. REPORTING RESPONSIBILITIES

6.1. Fraud Investigation results will not be disclosed or discussed with anyone other than those who have a legitimate need to know as agreed by the Fraud Response Group. Where possible, the Designated Person will acknowledge the concern to whoever reported the suspected Fraud and will confirm that the matter will be investigated. No other details will be provided due to confidentiality. In cases where an individual is suspected of Fraud, which a subsequent investigation does not substantiate, it is important that the potential damage to the individual's reputation is minimised.

At various stages in the process the University has a responsibility to notify the following bodies:

Audit & Risk Committee and Court

I. The Designated Person will notify the Convener of Audit & Risk Committee, at the earliest stage, when an investigation under the Plan has been initiated. The Convener of Audit & Risk Committee will also be informed of progress during any investigation and will be issued with a copy of the final report on the investigation. A formal report (as detailed above in paragraph 4.4) will normally be submitted to the next meeting of the University's Audit & Risk Committee. However, if the particulars of the fraud investigation are significant in value, novel, unusual or complex then a special meeting of the Audit & Risk Committee may be convened. Audit & Risk Committee will report to Court on matters considered and relevant management responses.

External Audit

II. The University has a duty to report all cases of fraud to its external auditors. The Head of Internal Audit should be responsible for this.

Police

III. The FRG is responsible for deciding whether and when it is necessary to inform the Police. The FRG will seek advice from the UCO, the Head of Legal Services and/or external Legal Advisors (as appropriate) when making a decision on whether or not to report a Fraud to the Police. The Convener of Audit & Risk Committee will be notified by the Designated Person of any such action.

Where the Police are not notified by the University of a suspected or actual case of Fraud, the Convener of Audit & Risk Committee will be advised of the reason. This is in compliance with Scottish Funding Council guidance.

All contact with the Police following their initial involvement will be via the Designated Person or a nominated, authorised substitute.

The Scottish Funding Council (SFC)

IV. The Principal is responsible for ensuring the SFC is informed of any, actual or suspected, significant Fraud, in line with the requirements of the Financial Memorandum. SFC should also be informed where there is likely to be public interest because of the nature of the fraud or the people involved.

Involvement of University Insurers

V. The Investigating Officer, in discussion with the Chief Financial Officer and the Insurance Manager, should decide, depending on the nature of the Fraud, whether any of the losses warrant a claim under any University insurance policy.

Involvement of Information Commissioner's Office

VI. The Data Protection Officer will determine whether the Fraud amounts to a data protection breach which requires to be reported to the Information Commissioner's Office and will advise the Designated Officer.

National Crime Agency

VII. Where the Fraud amounts to a case of money laundering, the FRG will ensure it is following the provisions of the Anti-Money Laundering Policy and will consult with the University's Money Laundering Reporting Officer with regards to making any reports to the National Crime Agency.

Other organisations

VIII. In certain circumstances, the University may have to report fraudulent activities to third party partners where the Fraud relates to the University's relationship with such partners, for example, Research Councils, Student Awards Agency for Scotland, Student Loans Company.

7. RECOVERY OF LOSSES

7.1. The Investigating Officer shall ensure that the amount of any loss is quantified wherever possible. Repayment of losses, where a case of fraud has been proven, will be sought in all cases.

Where the loss is substantial, legal advice should be obtained without delay about the need to freeze the suspect's assets through the appropriate court, pending conclusion of the investigation. Legal advice should also be obtained about prospects for recovering losses through the appropriate court, where the perpetrator refuses repayment. The University will normally expect to recover costs in addition to losses.

8. EXTERNAL FRAUDS

8.1. For the purposes of this section, “external frauds” are fraud perpetrated by third parties against the University.

If there is any suspicion of collusion on the part of staff or student(s) in a suspected or discovered external fraud, the procedures described in this Fraud Response Plan apply in full.

Where there is no suspicion of collusion on the part of staff or student(s), cases of suspected external fraud should be reported to the Designated Person. The Designated Person should notify the Fraud Response Group who will normally recommend to the Principal that the matter be reported to the Police or appropriate organisation.

9. REVIEW OF THE FRAUD RESPONSE PLAN

9.1. The Plan will be reviewed to ensure fitness for purpose periodically and after each incident to identify any need for change. Amendments will be approved by the Executive Team and the Audit & Risk Committee. Where proposed changes are substantial in nature, then Court approval will also be sought.

APPENDIX 2 – EXAMPLES OF FRAUD, SUSPICIOUS ACTIVITY AND BEHAVIOURAL INDICATORS

Examples of **Fraud** include, but are not limited to, the following:

- Misappropriation of cash e.g. theft of cash from cash boxes, cash registers, and takings from trading outlets, vending machines, or from social funds;
- Theft of stock;
- misuse of any University funds;
- Fraudulent encashment of payable orders or funds;
- Misuse of University fuel cards;
- Misappropriation of other assets including information and intellectual property. This would also include theft of stationery or other University property for private use, unauthorised use of University property e.g. vehicles, computers, other equipment;
- Purchasing or purchase ledger fraud (e.g. approving/paying for goods not received by the University, approving/paying bogus suppliers, approving/paying inflated prices for goods and services, accepting any bribes);
- Colluding with suppliers of the University to defraud the University of funds and/or good/services;
- Cyber theft via cyber-phishing emails or user impersonation which can lead to theft of financial resources and/or personal data;
- Travel and subsistence claims overstated or falsely claimed. This may include advances not recovered or forging of counter-signatories;
- Accepting pay for time not worked (e.g. false claim for hours worked, failing to work full contracted hours by any member of staff, false overtime claims, or falsification of sickness self-certification) and/or retaining payments made by the University in error;
- Cyber Fraud (e.g. altering or substituting records, duplicating or creating spurious records, theft of personal data or destroying or suppressing records);
- Fraudulent financial reporting e.g. improper revenue recognition, inflating asset value, understating liabilities and provisions;
- Deliberate misrepresentation of information, e.g. personal, educational, research data, recruitment data, academic credentials, and/or financial circumstances for the purpose of obtaining a benefit;
- Identity fraud;
- Presentation of fraudulent documents in an application for admission or employment or as part of a University process;
- Deliberate misuse of a third party's identity for the purposes of obtaining a benefit;
- Falsification of documents;
- Bribery, corruption & undue influence in University decision-making;
- deliberate circumvention of University procurement guidance;
- serious deviations from University policy without a clear justification;
- making false statements or representations;
- dishonestly failing to disclose information;
- dishonestly abusing a position;
- fraudulent trading or dishonestly obtaining services;
- money laundering (See the University's Anti-Money Laundering Policy for more information).

Suspicious activity may include, but is not limited to, unusual transactions, unexplained changes to records or processes, behaviour inconsistent with expected roles or controls, or attempts to bypass established procedures. These indicators do not in themselves prove fraud but may warrant further review. Examples include but are not limited to, the following:

- Unexplained change requests to bank details
- Pressure to bypass procurement procedures
- Pressure to make urgent payments
- Requests to override standard data entry
- Complaints from student over misrepresentation of courses or fees
- Use of undisclosed sub-contractors
- Circumvented procedures
- Pressure to reclassify costs to meet funder requirements
- Requests to backdate approvals
- Undisclosed conflicts of interest
- Refusal to take annual leave

A list of Behavioural indicators is set out below, which is not exhaustive, which may assist staff in identifying possible signs of Fraud and suspicious activity. Some of the examples on this list could be an indicator of Fraud or suspicious activity but may also highlight wellbeing issues and as such should be addressed with sensitivity. Some examples taken in isolation may not be an indication of fraudulent behaviour but when taken with other examples could raise suspicion.

- Management override of controls;
- Missing or altered documents to support prices / fees payable and receivable;
- Prime documents being lost and replaced by photocopies;
- Charges being made for goods or services not supplied or ordered;
- Credits or refunds without appropriate authorisation and documentation;
- Changes in normal patterns for example travel claim details;
- Delay in completion or submission of claim forms;
- Lack of vouchers or receipts in support of expense claims, including purchases made through purchase cards and travel cards;
- Staff seemingly living beyond their means;
- Individuals using assets of Strathclyde, including the name, for personal gain without proper authorisation or reimbursement for their use;
- deliberate circumvention of University procurement guidance;
- ‘suspicious activity’ or ‘red flags’ which includes actions or patterns that may suggest the potential for fraud or misconduct but lack conclusive evidence of fraud
- Staff under constant financial or other stress;
- Reluctance of staff to take annual leave (and so preventing others becoming involved in their work), especially if solely responsible for a 'risk' area;
- Complaints from public or staff;
- Avoidance of audits or peer reviews (internal or external);

- Always working late;
- Refusal of promotion;
- New staff resigning quickly;
- Suppliers/contractors insisting on dealing with a particular member of staff;
- Strathclyde staff with conflicts of interest with suppliers/contractors/customers/collaborators;
- Payments for tuition fees from multiple credit cards by third parties not apparently connected to the student;
- Repeated applications for hardship or emergency funds with limited supporting documentation or refusal to provide further explanation or documentation on request;
- Fraudulent references for admissions;
- Apparent and significant discrepancies between a students' professed qualifications and knowledge and how these are displayed in learning and teaching activities;
- Sudden changes in behaviour.

APPENDIX 3 – WHAT TO DO AND NOT DO IF YOU SUSPECT FRAUD

What to do:

- Report your concerns, reports will be treated discreetly and will remain as confidential as possible (see Sections 7.11 -7.14 for guidance on who to report to);
- Stay calm - remember you are a witness not a complainant;
- If possible, write down your concerns immediately - make a note of all **factual** events and discussions such as what was said in phone or other conversations, the date, the time and the names of anyone involved;
- Keep or copy any document that arouses your suspicions. This retains documents for use in any subsequent investigation and avoids any documents being accidentally - or purposely – destroyed;
- Make sure that your suspicions are supported by facts, as far as is possible at this stage;
- Be discreet with the information, only discuss it with the nominated individual (as noted in Sections 7.11-7.14) or people they refer you to;
- Be responsive to staff concerns;
- Deal with the matter promptly;
- Don't be afraid to seek advice from an appropriate person.

What not to do:

- Don't keep quiet and hope the problem will go away;
- Don't become a private detective and personally investigate or conduct interviews;
- Don't approach the person/persons potentially involved (this may lead to conflict, violence, destruction of evidence etc.);
- Don't discuss your suspicions or case facts with other staff or colleagues;
- Don't contact the police directly - that decision is the responsibility of senior University officers;
- **Don't, under any circumstances**, **suspend anyone, if you are a Line Manager, without direct advice from the Chief People Officer or nominee;**
- Don't use the process to pursue a personal grievance.

APPENDIX 4 – FRAUD INVESTIGATION CHECKLISTS

Fraud Investigation - Checklist for Line Managers

The following is a checklist of points for consideration following the reporting of an alleged Fraud to line management.

- Do not rush in - consider all options and plan the approach;
- Establish as many facts as possible without alerting anyone;
- Maintain confidentiality;
- Make an immediate note of everything reported. Repeat these notes to whoever the report is being made to, to ensure clear understanding;
- Take steps to minimise any immediate further losses but **do not, under any circumstances**, **suspend anyone without direct advice from the Chief People Officer or nominee;**
- Secure any evidence;
- In line with Sections 7.11 - 7.14 of the Policy, inform the Head of Department/ School or Director or, where appropriate the Executive Dean/Senior Officer or a member of the Fraud Response Group.

Fraud Investigation - Checklist for Fraud Response Group

The following is a checklist of points for consideration following the reporting of an alleged Fraud to the Designated Person or a member of the Fraud Response Group.

- The Fraud Response Group convenes to consider the allegation(s);
- Keep a record of timelines and actions;
- Initial fact-finding investigation to establish substance of allegation(s);
- Consider legal implications;
- If appropriate, inform the Principal and Convener of Audit and Risk Committee;
- Agree if further investigation is required and who will undertake it;
- Agree a remit, establish scope of investigation and reporting deadlines;
- Ensure investigating officer has adequate resources and full access to staff, data and documentation;
- Ensure existing staff or student disciplinary policies are followed;
- Secure any evidence;
- Inform Police, Auditors, SFC, other regulatory bodies as appropriate;
- Hold regular progress meetings at which progress and agreed action is documented;
- Prepare the final report for Audit & Risk Committee.

The Fraud Response Group's immediate task is to decide the nature of the initial action. The nature of the action required will vary depending on the individual circumstances. However, the initial action will generally include the following:

- Consider whether a fact finding investigation is required to establish the facts and if so agree the scope and nature of any investigation to be undertaken;
- Consider what action is necessary to secure records / assets and prevent further loss;

- Consider the need to include in the membership of the Fraud Response Group representatives from other areas, including specialist areas such as Information Services Directorate, Estates Services, Insurance Services, Information Governance Unit, appropriate student representation and the appropriate Executive Dean / Senior Officer of the area in which the employee(s) under investigation is / are employed;
- Commence a dedicated action log/tracker and set up a SharePoint site (or equivalent) to maintain records relating to the incident;
- Consider whether to request specialist services from the University's insurers;
- Seek expert legal advice from the University's external solicitors, if required;
- Consider the need to contact the Scottish Funding Council, the Police, Information Commissioners Office, Student Awards Agency Scotland, UK Visa Compliance and/ or other external bodies;
- Based on the information currently available and in discussion with the Cyber Security Manager, whether the incident meets the criteria for a cyber incident. If so, determine if a Cyber Incident Response Team needs to convene to commence an initial investigation and assessment, then contain and isolate the cyber incident from the corporate network;
- Relevant information to be shared with Head of Communications and Marketing to enable any press enquiries or social media postings to be responded to effectively. It may be appropriate for the Head of Communications and Marketing to attend the Fraud Response Group;
- Agree a timetable for completion of the initial action;
- Date of next meeting of the group.

Subsequent meetings of the Fraud Response Group:

- Determine and assign further actions required.
- Monitor progress of investigation & associated agreed actions
- Where appropriate support for staff who have had their personal details compromised e.g. enhanced credit checks.
- Designated Officer determines when the incident is over and instructs a lessons learned review to be carried out. This is to identify any areas for improvement in the incident response process. The Designated Officer will ensure any recommendations arising are closed out.

A record of each meeting, agreed actions and responsible persons should be documented by the Designated Person or nominee.

APPENDIX 5 – FRAUD REPORTING FLOWCHART

Initial Disclosure

- The individual should disclose their concerns to fraud-reporting@strath.ac in the first instance. If this is not appropriate, the concern should be disclosed to the appropriate senior person in line with Clauses 7.11-7.14 of the Counter Fraud Policy.
- In exceptional circumstances, the individual can disclose their concerns to a member of the Fraud Response Group or the Convenor of the Audit & Risk Committee (ARC)
- If staff feel unable to follow these fraud reporting processes, then they can use the University's Public Interest Disclosure (Whistleblowing) Policy and Procedures

Initial Suspicion

- The individual who suspects fraudulent activity should document their concerns noting all relevent details such as dates, times and individuals concerned.
- The individual should keep or copy any information that aroused suspicion.
- The individual should be discreet about their concerns and deal with the matter promptly.

Referall to UCO

- The Line Manager should report the matter to the Head of Department / School or PS Director.
- The Head of Department / School or PS Director should report the matter without delay to the University Compliance Officer.
- Where the concern has been disclosed directly to the Executive Executive Dean / Senior Officer, they should report the matter without delay to the University Compliance Officer.

Fraud Response Group

- The Designated Person (UCO) will convene a meeting of the Fraud Response Group.
- The Fraud Response Group will meet to assess the information and consider the appropriate action, considering legal implications.
- The Fraud Response Group will document its decision and the agreed action to be taken.

Investigator Appointed

- The Designated Person will appoint an Investigating Officer, usually the Head of Internal Audit.
- The Fraud Response Group will agree the remit of the Investigating Officer and the scope of the investigation. The Designated Person shall inform the Convener of Audit & Risk Committee and the Principal and keep them regularly updated on the matter.
- The Fraud Response Group will ensure that the Investigating Officer has access to the necessary resources, data and documentation.

Fact Finding Inestigation

- The Investigating Officer will conduct a preliminary fact finding investigation and produce a preliminary report for consideration by the Fraud Response Group.
- Where the preliminary fact finding investigation does not substantiate the suspicions of fraud, the Designated Person will inform the individual that initially reported the concerns that no wrongdoing has been uncovered.
- Where the preliminary fact finding investigation indicates that there may be fraudulent activity, a decision will be taken regarding whether the employee/s should be suspended and the FRG will decide next steps in accordance with Section 3.3 of the Plan.

Further Investigation

- The Fraud Response Group will determine and document the parameters of any substantive investigation with the Investigating Officer or shall refer to another Policy in accordance with Section 3.3 of the Plan.
- The relevant Investigating Officer will conduct the in-depth investigation or investigation under relevant Policy or Procedure and produce a final report for the Fraud Response Group.
- The Designated Person will inform the Principal and the Convenor of ARC of the findings of the investigation.

Disciplinary Procedures

- If the investigation finds there is a case to answer, the Designated Person will invoke the University's Disciplinary Procedures if not already involked.
- Where this applies to staff, the Chief People Officer or their nominee will take responsibility for conducting the Staff Disciplinary Procedure.
- Where this applies to students, the Director of Student Experience will take responsibility for conducting the Student Disciplinary Procedure.

Remediator

- The Investigating Officer shall ensure that the amount of loss is quantified where possible. Where fraud has been proven, the University will seek to recover these losses from the perpetrator of the fraud.
- Where the loss is substantial, the Designated Person will seek legal advice regarding the need to freeze the suspect's assets or recovering the losses (and additional costs) via the civil court.

Review

- The Fraud Response Group will conduct a review to understand whether any lessons can be learned to prevent the reoccurence of the fraudulent activity.
- This will include identifying any weaknesses in the internal control environment and highlighting any deficiencies in the systems for reporting and investigating.

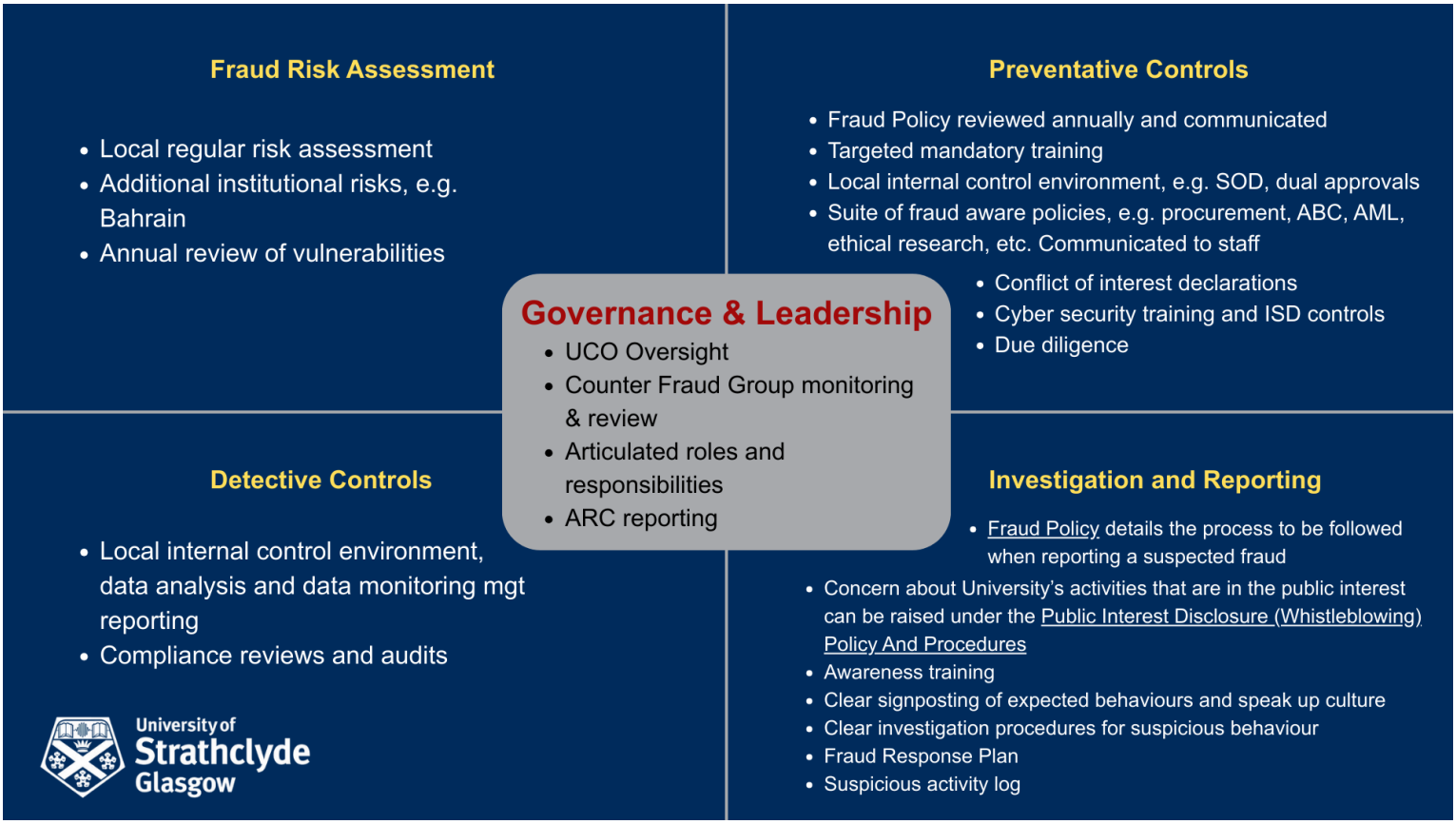
Reporting

- The Fraud Response Group will prepare a report for the ARC for onwards reporting to the University Court.
- The Fraud Response Group will report the fraud to the University's External Auditors via the Head of Internal Audit.
- The Fraud Response Group will consider the requirement for further reporting to the Scottish Funding Council, the University's insurers and the Police.

APPENDIX 6 – FURTHER REFERENCE

- Anti-Bribery and Corruption Code of Conduct
- Policy for the Offering or Receipt of Gifts, Hospitality and Other Benefits
- Public Interest Disclosure
- Conflicts of Interest – Code of Practice
- Expenses Policy
- Travel Policy
- Financial Regulations
- Anti-Money Laundering Policy
- PCI DSS Guidance
- Procurement Guidance
- Sickness Absence Management Policy
- University Procedure in relation to Work for Outside Bodies including Consultancies
- Information Services Policies & Regulations
- Information Security Policy
- Scottish Funding Council
- Internal Audit Service
- Staff Appointment Protocols
- Intellectual property
- Staff Disciplinary Procedure
- Student Discipline Procedures

APPENDIX 7 – FRAUD RISK MANAGEMENT FRAMEWORK



APPENDIX 8 – CORE ROLES AND RESPONSIBILITIES OF FRAUD RESPONSE GROUP

A. Initial Assessment and Triage

- Receive and assess allegations or suspicions of fraud
- Determine **credibility, severity, and urgency**
- Decide whether the issue meets the threshold for formal investigation

B. Investigation Oversight

- Decide **how the investigation will be conducted**
- Appoint investigators and define scope
- Ensure:
  - Evidence integrity
  - Confidentiality
  - Fair treatment of individuals involved
  - Avoid conflicts of interest

C. Legal and Regulatory Management

- Assess legal obligations, including:
  - Reporting to regulators, funders, or law enforcement
  - Employment law considerations
  - Data protection and privacy requirements
- Coordinate legal advice to reduce liability and procedural risk

D. Decision-Making and Sanctions

- Review investigation findings
- Recommend or approve:
  - Disciplinary action
  - Contractual remedies
  - Referral to police or regulators
  - No further action
- Ensure decisions are proportionate and defensible

E. Financial Recovery and Loss Management

- Quantify losses
- Support:
  - Asset recovery
  - Insurance claims
  - Restitution processes
- Prevent further losses during the response phase

F. Communication and Reputation Management

- Control internal and external communications
- Decide:
  - Who needs to know
  - What can be disclosed
  - When disclosures occur
- Protect organisational reputation while meeting transparency obligations

G. Learning and Prevention

- Identify control weaknesses exposed by the fraud
- Recommend improvements to:
  - Policies and procedures
  - Internal controls
  - Training and awareness
- Feed lessons learned into the organisation's Fraud Risk Management Framework

APPENDIX 9

PROTOCOL FOR UNDERTAKING INVESTIGATIONS UNDER THE COUNTER FRAUD POLICY ANNEX TO FRAUD POLICY

INTRODUCTION

Under the Fraud Response Plan set out in Appendix 1 of the Counter Fraud Policy, the Fraud Response Group (FRG) will normally appoint an Investigating Officer to undertake the investigation. Prior to any such investigation, the Investigating Officer shall undertake the training set out in this Protocol and agree to follow the guidance contained within this Protocol.

Upon appointment, the Investigating Officer may be instructed to conduct a preliminary fact-finding investigation to enable the facts of the circumstance to be investigated in a manner which is both rigorous and timely and maintains strict confidentiality subject to the need to share information with appropriate members of staff or external organisations.

The Investigating Officer should produce an interim report, for consideration by the FRG, which will provide sufficient detail to allow an assessment to be made as to whether a fraud has occurred. The interim report should:

1. set out the findings to date;
2. set out the interim conclusions drawn from those findings; and
3. set out an action plan to continue the investigation, if this is considered appropriate.

The FRG will consider the interim report and agree in writing on whether:-

1. A substantive fraud investigation should proceed; or
2. An investigation under another University Policy or Procedure should proceed which may require different investigating officers to be appointed; or
3. The matter should be concluded based on the findings of the interim report.

The FRG shall continually review progress being made on the investigation, to verify that the Investigating Officer is receiving the support and information they require and to ensure that the investigation will conclude as soon as possible.

Prior to initiating any investigation the following requirements will be followed:

TRAINING REQUIREMENTS

1. If not already done so, undertake BUFDG Intro to Counter-Fraud training
2. Review Managing Investigations Presented by Anderson Strathern.pptx available via the Complaints Handling Sharepoint
3. Engage with Legal Service around specific investigator training

FURTHER REQUIREMENTS

1. Following appointment as Investigating Officer a meeting will be set up with the Investigating Officer, University Compliance Officer (UCO) and Head of Legal and, depending on the nature of the allegations, the Assistant Director - Employee Experience; Deputy Director of Finance Operations; Head of Safeguarding and/or Head of Student Advice and Support in order to agree on:-

   A. the remit, scope, related timeline , noting that there should not be any unreasonable delay, and reporting requirements (including report recipient) of:-
      (i) the initial fact-find investigation (to be documented and agreed); and
      (ii) where required, the substantive investigation (to be documented and agreed); and
      (iii) where required, any investigation to be undertaken under any other University Policy or Procedure.

B. the support to expect from the FRG and other appropriate professional colleagues across the University with specialist expertise e.g. procurement, ISD, legal, HR finance, when undertaking an investigation;
C. the scope of their remit with regard to being able to request information, data, professional services support and access to employees;
D. The requirements with regards to reporting conclusions of the relevant investigation to the FRG.

2. The Investigating Officer will acknowledge their responsibility to maintain confidentiality and integrity noting that information may need to be shared with appropriate members of staff or external organisations within the scope of the investigation. The Investigating Officer will acknowledge that impartiality is crucial throughout the investigation and, should any perceived or actual conflict of interest arise during the investigation, the Investigating Officer will immediately advise the UCO, whom failing the Chief Financial Officer, whom failing the Chief People Officer who will consider the matter in line with the Fraud Policy and the Code of Practice on Conflicts of Interests.

3. The Investigating Officer will acknowledge their obligations of independence, not to be influenced by colleagues in their pursuit of facts, conclusions and recommendations. Where the Investigating Officer believes that there has been an attempt to influence the investigation in any way, they will immediately advise the UCO, whom failing the Chief Financial Officer, whom failing the Chief People Officer who will consider the matter in line with the Fraud Policy and other relevant University polices.

4. At any point during the investigation where the Investigating Officer believes that they do not possess the correct skillset to undertake the investigation, they will immediately advise the UCO, whom failing the Chief Financial Officer, whom failing the Chief People Officer and the matter will be considered at a meeting of the FRG.

5. The Investigating Officer will plan the investigation and keep that under review.

6. The Investigating Officer will update the UCO on a two-weekly basis of progress of the investigation.

7. Generally, preliminary investigation / scoping interviews should be distinguished from any employment or disciplinary interviews. It is generally accepted that an early witness interview can assist in clarifying the situation and may negate any further investigative process from being required, saving a substantial amount of time and resource and causing less anxiety for those involved. Conversely, the Dignity and Respect Policy and Staff Disciplinary Procedure both note that a member of staff is entitled to be accompanied in any formal interview situation by a Union representative or other colleague. Where the accused is a member of staff, it may be helpful to gain clarification of processes / incidents and interview certain members of staff which may include the accused and/or their line management at an early stage under a fact-finding investigation. In these circumstances, the Investigating Officer should partner with an HR representative to ensure that any investigative interview would not impinge upon a future Staff Disciplinary matter and ensure the matter was investigated under Dignity and Respect principles. In addition, care would need to be taken if the accused is to be interviewed to avoid any tipping off as this could compromise the investigation, for example, possible destruction of evidence. In these circumstances, advice should be taken from appropriate members of staff e.g. UCO, Head of Legal Services, Assistant Director - Employee Experience.

8. Where the accused is a member of the student population, it may be helpful to gain clarification of processes / incidents and interview the accused at an early stage under a fact-finding investigation. In these circumstances, the Investigating Officer should partner with the Head of Safeguarding and/or Head of Student Advice and Support to ensure that any investigative interview would not impinge upon a future Student Disciplinary matter and ensure the matter was investigated under Dignity and Respect principles. As noted above, care would need to be taken if the accused is to be interviewed to avoid any tipping off as this could compromise the investigation, for example, possible destruction

of evidence. In these circumstances, advice should be taken from appropriate members of staff e.g. UCO, Head of Legal, Assistant Director - Employee Experience.

9. The Investigating Officer will acknowledge that there may be safeguarding and/or wellbeing issues which they become aware of during the investigation. In such instances, the Investigating Officer shall immediately advise the UCO, whom failing the Chief Financial Officer, whom failing the Chief People Officer who will consider the matter in line with appropriate University policies and procedures.

10. Following conclusion of the full investigation, there will be a lessons learned meeting with the FRG, the Investigating Officer and any other relevant members staff to discuss any lessons learned from the investigation and improvements that can be made for future investigations under the Fraud Policy. Such meeting will be minuted, any lessons noted in the Suspicious Activity Log and the FRG shall ensure that any agreed actions are implemented.