University of
Strathclyde
Glasgow

Fraud Policy

Policy Owner	Date of latest review	Approval	Effective Date
University Compliance Officer	May 2023	Executive Team/ Audit & Risk Committee/ Staff Committee	October 2023

Fraud Policy
Contents

1. INTRODUCTION

1.1. 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 Fraud Policy (the "Policy") is a public statement of the University's resolve to prevent, detect and act upon cases of fraud 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, including cyber fraud. An anti-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 disbursement of public monies. All staff should undertake cyber security training to ensure they are up to date with current approaches to minimizing fraudulent attempts to acquire University financial resources and personal data.

1.3. The University Compliance Officer (UCO) is the Designated Person with responsibility under the Policy.

2. DEFINITION

2.1. For the purpose of this Policy, fraud may be defined as an intentional act involving the use of deception in order to obtain an undue benefit or avoid an obligation that results in a loss to another party.

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, concealment of material facts and collusion.

Under this Policy, intent is central to the University's understanding of fraud regardless of whether actual gain or loss has occurred. It should be noted that fraud may be perpetrated by individuals internal or external to the University.

2.2. Examples of fraud, which are neither exclusive nor exhaustive, include 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;
- Fraudulent encashment of payable orders, funds or cheques;
- Misappropriation of other assets including information and intellectual property. This would also include theft of stationery 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 personal, educational and/or financial circumstances for the purpose of obtaining a benefit;
- 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.

3. SCOPE

3.1. This Policy is applicable to all staff, students and applicants of the University, agents and other volunteers / lay members. Any fraudulent activities identified in relation to other individuals working with, or on behalf of, or for the University should be reported through the same process. 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 policies.

3.2. The University takes any allegations of fraud seriously and will investigate all such concerns. Staff members or student 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, where relevant.

4. STRATEGIC APPROACH

4.1. The University has a zero-tolerance policy towards fraud whether that is actual or attempted. 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 the Fraud 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 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.

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 and senior managers should therefore ensure that their behaviour always adheres to the highest principles of probity.

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 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 reserves the right to operate more than one policy at a time, where appropriate; for example, and without limitation, in respect of Fraud, the staff Disciplinary Procedure may be utilised in conjunction with the protocol defined within this Policy. Suspected fraudulent acts undertaken by a student may be referred for action under the University's Student Discipline Procedure and may be reported to the police or to other relevant organisations, e.g. Student Awards Agency Scotland.

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 5 Further Reference section.

Internal Audit Services

5.6. 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.

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 to comply with employment law; and

- Essential qualifications should be checked before making an offer of employment such as requiring original certificates prior to commencing employment.

Cash Handling Procedures

5.8. These should be clearly defined and communication supported by segregation of duty controls to prevent one person from receiving, recording and banking cash / cheques. In addition, a full audit trail of cash / cheque transactions should be maintained through the documentation of receipts.

Physical Security

5.9. All cash and assets (including valuable data) should be kept and stored securely with clear access rights defined and implemented.

Budgetary Control

5.10 Budget Holders should be alert to the risk of fraud or loss when monitoring actual income and expenditure against budget.

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 to report suspicion or detection of any incidence of fraud at the earliest opportunity.

6.2. Internal management systems are important measures because the risk of processing an irregular transaction is minimised where transactions are reviewed systematically. 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.

Warning signs

6.3. The following list of behavioural indicators, which is not exhaustive, may assist staff in identifying possible signs of fraud. Some of the examples on this list could be an indicator of fraud or irregularity 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 cash takings or 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;
- 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;
- 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.

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. The Code of Practice on Conflicts of Interest also requires certain members of staff to submit an annual declaration of interests. 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 should understand the risk of fraud faced by the University. Fraud is serious and diverts resources away from the University's primary objectives. It is the responsibility of all staff to be fraud aware and take the necessary steps to minimise the risk to the University.

7.4. All staff are responsible for:

- Acting with propriety in the use of University resources and in the handling and use of University funds, whether they are involved with cash or other forms 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;
- Reporting details immediately in accordance with Sections 7.10-7.13 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.

7.5. 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.

7.6. 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.

7.7. 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.

7.8. 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. A summary procedural flow chart is included in Appendix 4 and Appendix 2 gives useful pointers on what to do or not to do for anyone who suspects a fraud has occurred or is occurring.

Notification of Suspected Fraud

7.9. Anyone having reasonable suspicion of fraud should report it immediately in accordance with the sections below, knowing that their suspicions will be treated in strict confidence. No employee or student will be disadvantaged in any way as a result of reporting reasonably held suspicions. However, this assurance is not extended to someone who maliciously raises a matter they know to be untrue or should reasonably have known to be untrue.

7.10. Suspicions should be raised in the first instance with the immediate Line Manager or, should the Line Manager be the subject of suspicion, the next most appropriate senior person. In the case of suspected student fraud, suspicions should be raised with the line manager or service: for example:

In relation to applications for hardship or emergency funds, or statutory student funding (e.g. Student Awards Agency Scotland awards) – the Funding and Financial Support Manager or Head of Student Support and Development.

In relation to admissions - the Admissions Team in the relevant Faculty, Head of Department, and/or Student Experience Admissions Team and (in the case of international students) the Visa Compliance Team and/or the Recruitment & International Office.

In relation to tuition fee payments or other payments to the University: the Deputy Director of Finance (Operations).

A concern may also be raised through Report and Support if it is not clear where to route the concern.

Students may also raise a fraud concern, whether relating to students or staff, through Report and Support.

7.11. The Line Manager should then raise the matter with the Head of Department / School or PS Director. If the Head of Department / School or PS Director is subject to suspicion then the matter should be raised directly with the Executive Dean / Senior Officer. The Head of Department / Director / Executive Dean / Senior Officer should raise the matter with the Designated Person, who has the authority to invoke the Fraud Response Plan. Where there are also suspicions of breaches of cyber security or a cyber-attack, the IT Helpdesk must be contacted at the earliest opportunity. Similarly, if there are suspicions of theft of personal data then the Data Protection must be contacted at the earliest opportunity.

7.12. In exceptional circumstances, where it is inappropriate to follow the routes above, the disclosure can be made directly to a member of the Fraud Response Group (the UCO, Chief People Officer, Chief Financial Officer, Head of Legal Service and the Head of Internal Audit) or the Convener of the Audit & Risk Committee.

7.13. If staff feel unable to follow these fraud reporting processes, then they can use the University's Public Interest Disclosure (Whistleblowing) Policy or contact Protect, the free, confidential whistleblowing advice service 020 3117 2520. Or they may visit the Protect website.

7.14. The Public Interest Disclosure (Whistleblowing) Policy provides a mechanism whereby staff may report concerns in confidence without their identity being disclosed and interfaces with this Policy but is not the same. 'Whistle blowing' can relate to a whole range of ethical and academic matters.

7.15. Senior Officers, Executive Deans, Heads of Department/Schools, Directors Line Managers and any staff member to whom a suspected fraud is reported should note that suspects have certain rights under University policy and **no action** (such as interviewing staff) should be taken without prior consultation with the University Compliance Officer. Failure by University staff to follow established procedures in relation to investigating fraud and interviewing the staff involved can invalidate disciplinary action and compromise the success of any investigation and / or prosecution. Appendix 3 contains a checklist of points for consideration following the reporting of an alleged fraud to line management.

Appendix 1 Fraud Response Plan

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

1. INTRODUCTION

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.

1.2. If any suspected fraud directly involves an officer referred to in this Plan, then the relevant reference should be replaced by a Senior Officer nominated by the Principal.

2. INITIATING ACTION

2.1. Suspicion of fraud may be captured through a number of means. As examples, an irregularity may come to light as a result of an employee, student or member of the public raising concerns, an Internal Audit review or an External Audit review. All cases of suspected or known fraud should be reported immediately, regardless of the apparent amounts involved, to the University Compliance Officer (the Designated Person).

2.2. Where required, the Designated Person should convene a meeting of the University's Fraud Response Group as soon as possible. The Fraud Response Group consists of the Designated Person (Convener), Chief People Officer, Chief Financial Officer, the Head of Legal Services and the Head of Internal Audit. Depending on the type of suspected Fraud, the Designated Person may invite additional members of staff to join the Fraud Response Group, for example, the Chief Digital and Information Officer in the event of suspected cyber fraud or the Data Protection Officer in the event of suspected theft of personal data. In the absence of any member of the Fraud Response Group specified, a nominated depute shall attend. As a general rule the number of people to be involved at this stage should be minimised. In the case of suspected student fraud, the University Compliance Office will consult with the Director of Student Experience, Director of Finance and/or Head of Internal Audit and such other relevant members of staff (as appropriate) to determine whether the Fraud Response Group 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. 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'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 an 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, 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 Chief Digital & Information Officer, 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.
- 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 identified 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.

2.4. After consultation with the Fraud Response Group, the Designated Person should appoint an Investigating Officer to take charge of the investigation. This will normally be the Head of Internal Audit. Where the Cyber Incident Response Team has also been convened, the Chief Digital Information Officer will keep the Fraud Response Group updated.

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

2.6. The Investigating Officer must conduct an initial "fact-finding" exercise 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 e.g. the Police, Scottish Funding Council, external Auditors.

2.7. The Investigating Officer should produce an interim 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 interim 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.

2.8. 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. 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. 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.

3. SUBSEQUENT INVESTIGATIONS

3.1. Where the initial investigation provides reasonable grounds for suspecting an employee(s) or student(s) 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 Director of Student Experience 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.

3.2. 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.

3.3. The Director of Estates / Head of Security Services should advise on the best means of denying access to the University whilst the employee/student remains suspended. The Director of Information Services 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.

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

3.5. The Investigating Officer shall consider whether it is necessary to investigate systems, other than that which has given rise to suspicion, through which the employee/student may have had opportunities to misappropriate the University's assets. The Investigating Officer will report any such concerns to the Designated Person.

3.6. As part of the internal investigation there may be a need to expand on the information collected as part of the initial fact-finding exercise so as to provide an appropriate level of evidence.

3.7. At the conclusion of the investigation a final report will be produced by the Investigating Officer. 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.

3.8. If the circumstances set out in the final report indicate that an employee/student has a case to answer, the Designated Person will invoke the University's internal disciplinary procedures.

4. CONCLUDING AN INVESTIGATION

4.1. At the end of a case, irrespective of the outcome, it is important that the progress of the investigation is reviewed to see what lessons can be learned 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 by a member of the Fraud Response Group in consultation with relevant line managers.

4.2. 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 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.

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

5. REPORTING OF FRAUD

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

Audit & Risk Committee and Court

5.2. The Designated Person will notify the Convener of Audit & Risk Committee, at the earliest stage, when an investigation under this procedure 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 4.2) 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

5.3. 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

5.4. It is the policy for the University to involve the Police, where appropriate, at an early stage of any investigation after an initial fact-finding review has been carried out. However, in certain investigations it may be more appropriate to wait until the internal investigation and final report has been completed by the Investigating Officer. The Convener of Audit & Risk Committee will be notified by the Designated Person of any such action.

5.5. 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 SFC guidance.

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

5.7. Where there is suspicion of a breach of cyber security then the Police should also be notified of this aspect of the fraud.

The Scottish Funding Council (SFC)

5.8. 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.

The Scottish Charity Regulator (OSCR

5.9. Any instance of fraud which has a significant impact on the University and/or the University reports to the Police must subsequently be notified to OSCR in accordance with its Notifiable Events Guidance. Prior to any such notification, the Designated Officer will first inform the Principal, the University Secretary and the Convener of Court.

Involvement of University Insurers

5.10. The Investigating Officer, in discussion with the Chief Financial Officer, should decide, depending on the nature of the case, whether any of the losses warrant a claim under any University insurance policy.

5.11. The assistance of the University's insurers may be requested to assist with managing any data protection breaches in an effective and co-ordinated manner. The Designated Officer in discussion with the Chief Financial Officer will decide whether this course of action is appropriate.

Involvement of Information Commissioner's Office

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

Requests for Information

5.13. Any requests for information from the press or anyone outside the University concerning any fraud investigation must be referred to the University Compliance Officer. Any statements to the media will be made by either the Head of Communications and Marketing or the Designated Officer.

5.14. Under no circumstances should the Investigating Officer or other manager / employee provide statements to the press or external persons. Making such statements is a contravention to this Policy and could result in disciplinary action.

Record Keeping

5.15. The Designated Person will keep a register of all reported concerns relating to fraud. The register 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.

6. RECOVERY OF LOSSES

6.1. 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.

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

7. EXTERNAL FRAUDS

7.1. External frauds are fraud perpetrated by third parties against the University.

7.2. 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.

7.3. 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.

8. REVIEW OF THE FRAUD RESPONSE PLAN

8.1. 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 - WHAT TO DO AND NOT DO IF YOU SUSPECT FRAUD

What to do:

- Report your concerns, reports will be treated as confidential (see Sections 7.10-7.12 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 relevant details 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 7.10-7.12) 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 3 - 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.

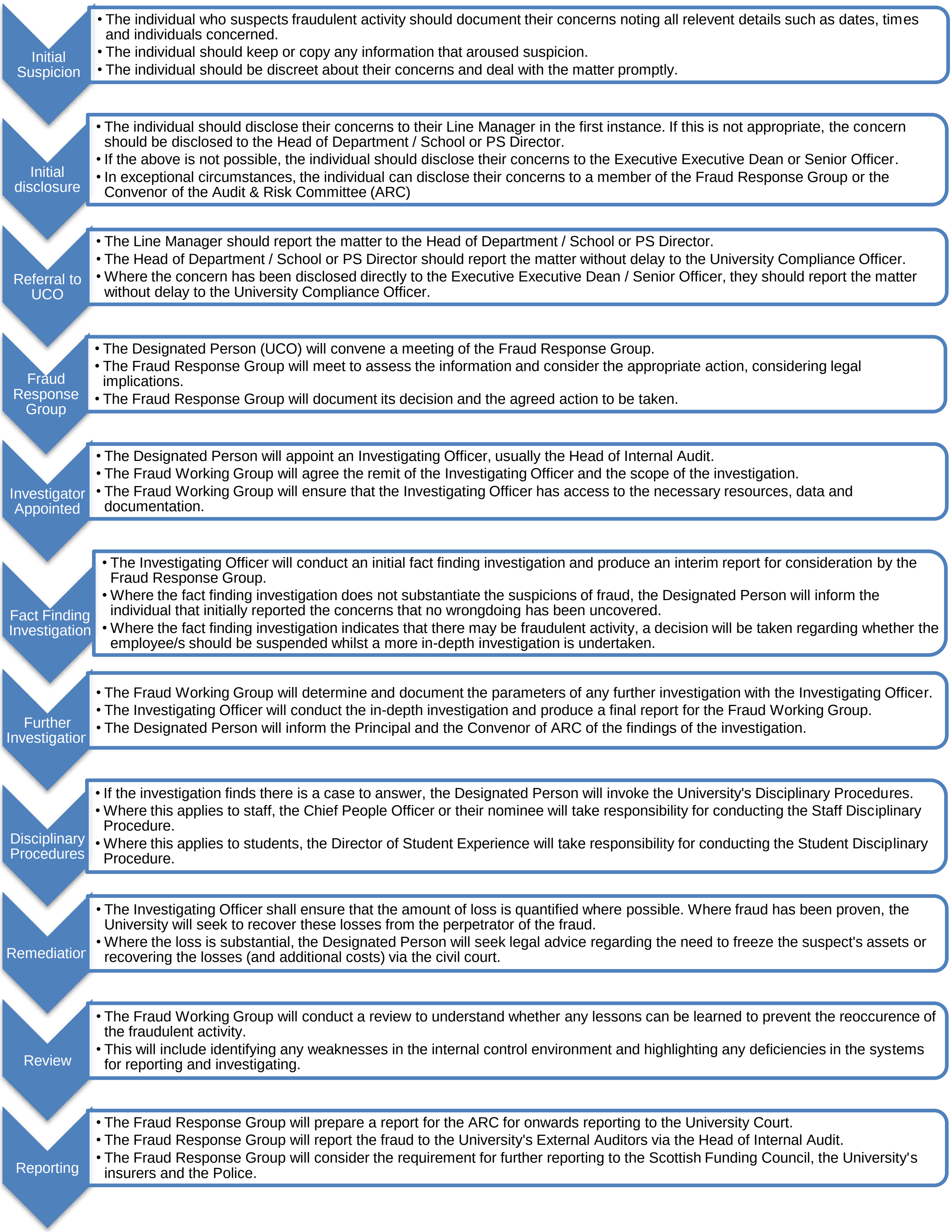
- Do not rush in - consider all options and plan the approach;
- Establish as many facts as possible without alerting anyone;
- Maintain confidentiality;
- Make an immediate note of everything reported. Repeat these notes to whoever is reporting the details to ensure clear understanding;
- Take steps 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;
- 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 as appropriate;
- Hold regular progress meetings at which progress and agreed action is documented;
- Prepare the final report for Audit & Risk Committee.

APPENDIX 4 - FRAUD REPORTING FLOWCHART



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.

Initial disclosure

- The individual should disclose their concerns to their Line Manager in the first instance. If this is not appropriate, the concern should be disclosed to the Head of Department / School or PS Director.
- If the above is not possible, the individual should disclose their concerns to the Executive Executive Dean or Senior Officer.
- 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)

Referral 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 Working Group will agree the remit of the Investigating Officer and the scope of the investigation.
- The Fraud Working Group will ensure that the Investigating Officer has access to the necessary resources, data and documentation.

Fact Finding Investigation

- The Investigating Officer will conduct an initial fact finding investigation and produce an interim report for consideration by the Fraud Response Group.
- Where the 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 fact finding investigation indicates that there may be fraudulent activity, a decision will be taken regarding whether the employee/s should be suspended whilst a more in-depth investigation is undertaken.

Further Investigatior

- The Fraud Working Group will determine and document the parameters of any further investigation with the Investigating Officer.
- The Investigating Officer will conduct the in-depth investigation and produce a final report for the Fraud Working 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.
- 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.

Remediatior

- 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 Working 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 5 - FURTHER REFERENCE

- Anti-Bribery and Corruption Code of Conduct: https://www.strath.ac.uk/professionalservices/media/ps/finance/forms/Anti-Bribery_&_Corruption_Code_of_Conduct.pdf

- Policy for the Offering or Receipt of Gifts, Hospitality and Other Benefits: https://www.strath.ac.uk/professionalservices/media/1newwebsite/documents/Policy_Receipt_Gifts_Hospitality_Other.pdf

- Public Interest Disclosure: https://www.strath.ac.uk/media/ps/comms/documents/Public_Interest_and_Disclosure_Policy.pdf

- Conflicts of Interest – Code of Practice: https://www.strath.ac.uk/media/1newwebsite/universitycourt/Conflicts_of_Interest_Approved_Sept_2018_with_Coversheet.pdf

- Expenses Policy: https://www.strath.ac.uk/media/ps/finance/expenseclaims/Expenses_Policy.pdf

- Financial Regulations: https://www.strath.ac.uk/professionalservices/media/ps/finance/financialregulations/Financial_Regulations.pdf

- Procurement Guidance: https://www.strath.ac.uk/procurement/procurementguidance/

- Sickness Absence Management Policy: https://www.strath.ac.uk/professionalservices/media/ps/humanresources/policies/Sickness_Absence_Management_Policy_published.pdf

- University Procedure in relation to Work for Outside Bodies including Consultancies: https://www.strath.ac.uk/media/ps/humanresources/policies/University_Procedure_in_relation_to_Work_for_Outside_Bodies_including_Consultancies_20052015.pdf

- Information Services Policies & Regulations: https://www.strath.ac.uk/professionalservices/is/policies/

- Information Security Policy: https://www.strath.ac.uk/is/cybersecurity/informationsecuritypolicy/

- Scottish Funding Council http://www.sfc.ac.uk/

- Fraud Act 2006 C.35 http://www.opsi.gov.uk/acts/acts2006/ukpga_20060035_en_1

- Internal Audit Service http://www.strath.ac.uk/internalaudit/

- Staff Appointment Protocols: https://www.strath.ac.uk/professionalservices/media/ps/humanresources/policies/Staff_Appointment_Protocols.pdf

- Intellectual property: https://www.strath.ac.uk/workwithus/strathclydeinspire/create/ipcommercialisation/intellectualproperty/