

# **Fraud Policy**

***April 2020***

# CONTENTS

Fraud Policy Statement	1
1. Procedure for Fraud Prevention, Detection and Investigation	2
1.1.Introduction	2
1.2. Fraud Prevention	2
1.3. Management Responsibility and Risk Management	3
1.4. Internal Controls	3
1.5. Management Checks	3
1.6. Staff/Training	4
1.7. Fraud Detection	4
2. Fraud Response Plan	5
2.1. Introduction	5
2.2. Reporting Fraud	5
2.3. Initial Enquiry	5
2.4. Prevention of Further Loss	6
2.5. Conducting a Fraud Enquiry	6
2.6. Recovery of Losses	7
2.7. Staffing Issues	7
2.8. Reporting During the Investigation	8
2.9. Concluding an Investigation	8
2.10.References for Employees Disciplined or Prosecuted for Fraud	8
Checklist for Line Managers	9
Checklist for the Fraud Investigation Group	9

# FRAUD POLICY STATEMENT

This University has a duty to its stakeholders to take all responsible steps to prevent fraud occurring, whether perpetrated by staff, students, contractors and suppliers, other organisations or members of the public. Cyber fraud in particular is increasing both in number and sophistication, as organised criminal gangs use this as a funding mechanism.

The University will maintain robust control mechanisms to both prevent and detect fraud. All line managers have a responsibility for maintaining documented control systems and must be seen to be setting an example by complying fully with procedures and controls. The effectiveness of controls will be subject to cyclical review by the University's Internal Auditors. In addition, training in cyber security is provided to all staff members.

All members of staff have a responsibility to protect the assets and reputation of the institution and are expected to be alert to the potential for fraud. Line managers should brief staff on the common types of fraud perpetrated in their areas of responsibility.

Confidential mechanisms have been established to allow staff to report suspected frauds to management. All reported suspicions will initially be investigated by the Fraud Investigation Group. The core members of such a group are:

- University Secretary & Chief Operating Officer (Chair)
- Chief Financial Officer
- Director of People
- Director of Digital & Information Services

Depending upon the nature of the fraud, other members may be brought in to assist the group and Internal Audit, or other specialist investigators, will be invited as appropriate.

Further information for staff on reporting fraud and their role in the prevention and detection of fraud is provided in the following procedure.

Note: a separate policy exists for dealing with research fraud.

# 1. Procedure for Fraud Prevention, Detection and Investigation

## 1.1. Introduction

The University's procedure for fraud prevention, detection and investigation is set out below.

The objectives of the procedure are to:

- encourage staff to be aware of fraud;
- bring suspected fraud to notice;
- provide a framework response plan for investigating and reporting fraud; and
- ensure both alleged and proven fraud are dealt with in a consistent and timely manner

The University has a unique role to play in the community and any instances of fraud or corruption may be damaging to public confidence and support. Losses due to fraud, theft or corrupt practices can have a direct effect on jobs and the level and quality of service provision. Data protection legislation places an increased responsibility on the University to secure personal data and fines of up to 4% of turnover can be imposed for a significant security breach. Vigilance is essential since all staff are responsible for ensuring that the best possible service is provided to the University's students and funders and that value for money is secured from public funds.

Successful fraud prevention involves creating an environment which inhibits fraud. Taking immediate and vigorous action if fraud is detected is not only necessary to prevent future losses, but also helps deter frauds. A manager who is alert to the possibility of fraud and who acts accordingly on a day-to-day basis is a powerful deterrent against fraud.

The University of Aberdeen has a 'zero tolerance' policy towards fraud, bribery and corruption. The University will always investigate and seek to take appropriate action, including [disciplinary](#) and/or legal action against those who commit, attempt to commit, or assist anyone committing fraud or any other improper activities in our operations.

## 1.2. Fraud Prevention

Fraud can be defined as 'any act of wilful dishonesty to gain individual or collective advantage'. It is taken to include theft, misuse of property, corruption, the alteration of financial or other records or any unauthorised act which results directly or indirectly in financial gain to the perpetrator or a third party. Fraud can be perpetrated against staff, students, suppliers, Government Agencies or Departments, or the public.

Staff should be aware that gifts, including hospitality, offered by contractors, suppliers and service providers may place employees in a vulnerable position.

Staff need to be increasingly aware of sophisticated “phishing” attacks which can allow entry into University systems or can divert payments unlawfully into fraudulent back accounts.

### **1.3. Management Responsibility and Risk Management**

The prime responsibility for preventing fraud lies with management through:

- identifying risks to which systems and procedures are exposed;
- designing, implementing, documenting and operating of internal controls;
- establishing an environment that promotes compliance with internal controls;
- promoting fraud awareness amongst staff; and
- fostering an ‘anti-fraud’ culture.

However, while managers are responsible for assessing and controlling the level of risk within their areas of authority, it is the responsibility of all staff to be aware of fraud and to take the necessary steps to minimise the risk to the University.

Managing the risk of fraud is the same in principle as managing any other business risk. It is best approached systematically both at organisational and operational level. Managers should identify risk areas, assess the scale of risk, allocate responsibility for managing specific risks and implement and test controls to minimise the risks.

Management also have a responsibility to familiarise themselves with common fraud techniques in areas for which they have control. Managers should also ensure that staff in their areas of operation are familiar with common types of fraud. Training is available for all staff on cyber security and the Information Champions will help increase awareness of cyber security threats in their areas.

### **1.4. Internal Controls**

Internal controls are the key element in preventing fraud. They include both financial and non-financial controls and those that are in place to safeguard the misuse of University assets, including IT systems. The financial regulations are one example of these controls. The University’s financial and other non-financial procedures are the definitive guide and are available to all staff. It is the responsibility of management to ensure that controls in their area of responsibility have been documented and communicated.

In order to set a good example, managers should be seen to be complying with all controls. The emphasis should be on creating a culture of honesty and fraud detection, not increasing the volume of detailed operational and supervisory checks and controls, unnecessarily.

### **1.5. Management Checks**

The prevention and detection of fraud and impropriety is only possible where strong internal controls are present and constantly applied. Routine checks and monitoring by management to ensure that procedures are being followed are, therefore, essential. The benefits of implementing a culture of strong management controls:

- a deterrent effect when it is known that management is actively involved in ensuring that procedures are followed, and

- the results of the checks will allow management to identify any operational areas where controls are not being uniformly applied and investigate whether systems have been exploited.

Management should regularly monitor compliance with controls and may also ask the Internal Auditors to test compliance. It should be emphasised that the prime function of internal audit is to evaluate the effectiveness of the overall framework of internal control, with management ensuring implementation and monitoring of the framework.

Common excuses for non-compliance with controls are that they are no longer applicable, insufficient time is available or they are not appropriate. It is important that such comments are reported to management so that the need for the controls can be re-evaluated.

## **1.6. Staff/Training**

Staff provide the best protection against fraud and corruption. It is important, therefore, that the University policy on fraud prevention and investigation is fully communicated to all staff. The lack of clear guidance and ignorance of procedures will often be the first excuse used by offenders.

The recruitment of suitable staff is the University's first defence in preventing fraud. Best practice recruitment policies such as detailed application forms including a statement on criminal records, communication with referees and past employers and verification of educational and professional qualifications will assist in this approach.

Staff awareness of policy and procedures is fundamental to the effective operation of systems. The University will comply with best practice, including:

- publication of University policy on fraud, corruption and impropriety including easy access to it for all staff;
- staff training including mandatory IT security training to assist with the avoidance and detection of cyber fraud;
- desktop instructions for specific tasks; and
- regular staff notices regarding changes to Financial Regulations and financial procedures.

## **1.7. Fraud Detection**

The primary responsibility for detecting fraud lies with management through the implementation, documentation and operation of effective systems of internal control. The University's Internal Auditors through their evaluation of the control framework also have a role to play in preventing and detecting fraud.

All staff have a responsibility to be aware of the potential for fraud and take the necessary steps to minimise the risk to the University.

Properly and consistently applied procedures for reporting and investigating fraud play an important part in preventing further fraud. The University expects that reported suspicions will be investigated. The University's fraud response plan set out in the next section must be implemented where fraud is suspected.

## 2. Fraud Response Plan

### 2.1. Introduction

Management and staff are likely to have little experience in dealing with fraud and when suspected cases arise, may be unsure of the appropriate action to take. The objectives of this response plan are:

- to provide a documented framework to which the University can refer in the event that fraud is suspected or reported; and
- to ensure that in the event of fraud, timely and effective action is taken to prevent further losses, identify fraudsters, safeguard evidence, minimise publicity, reduce adverse effects on the business and to learn lessons.

Fraud investigation checklists for line managers and the Fraud Investigation Group are attached.

### 2.2. Reporting Fraud

All actual or suspected incidents of fraud should be reported without delay to the Chief Financial Officer or other member of the Fraud Investigation Group. The core members are:

- University Secretary & Chief Operating Officer
- Chief Financial Officer
- Director of People
- Director of Digital & Information Services

When staff report suspected fraud it is important that their suspicions are treated seriously and that all details provided by the reporting employee are recorded accurately and in a timely manner. They should be repeated to the reporting employee to confirm understanding.

It is essential that staff are put at ease, since the decision to report the suspected fraud may be traumatic for the individual concerned. Staff (or others) reporting fraud should be assured that all information will be dealt with in the strictest confidence and that their anonymity will be preserved if requested, unless that is incompatible with a full and fair investigation.

Regardless of the direction any future internal or Police investigation may take, the anonymity of any 'whistle-blower' must be guaranteed during the initial investigation.

Having recorded the details of the individual case, the Chief Financial Officer should, within 24 hours, hold a meeting of the Fraud Investigation Group to decide on the initial response.

At this stage the management should also take whatever steps are necessary to prevent further losses e.g. by changing procedures or suspending payments – without compromising the quality of evidence or alerting the fraudsters.

### 2.3. Initial Enquiry

On receiving the details of the suspected fraud, the Fraud Investigation Group should undertake as limited review as necessary to establish whether further action needs to be taken. This may be an investigation, led by Internal Audit. If the fraud

involves a personal data breach, the University's Data Protection Officer will form part of the investigation group.

If this initial investigation suggests that suspicions are confirmed, the group will decide which body is best placed to undertake further investigative work and will inform the Principal, the Chair of the Audit Committee, the Senior Governor, auditors, the funding body and the Police as appropriate. The circumstances in which the institution must inform the funding body of actual or suspected fraud are set out in the funding body's audit code of practice. The Principal is responsible for informing the funding body of any such incidents.

#### **2.4. Prevention of Further Loss**

Where the initial investigation provides reasonable grounds for suspecting a member or members of staff of fraud, the Fraud Investigation Group will need to decide how to prevent further loss. Fraudulent or corrupt activity is regarded as a breach of contract and where there are reasonable grounds for suspicion then suspension, with or without pay, (consistent with the [disciplinary policy](#)) of the suspects is likely, pending the outcome of enquiries. The rights of staff on suspension must be acknowledged, for example their right to be accompanied to any disciplinary investigation/hearing.

It may be necessary to plan the timing of suspension to prevent the suspects from destroying or removing evidence that may be needed to support disciplinary or criminal action. Suspect(s) 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 institution. Any security passes and keys to premises, offices and furniture should be returned.

Advice should be obtained on the best means of denying access to the University while suspects remain suspended (for example by changing locks and informing security staff not to admit the individuals to any part of the premises). Similarly, access permissions to the University's computer systems should be withdrawn without delay.

The Group should consider whether it is necessary to investigate systems other than that which has given rise to suspicion, through which the suspect may have had opportunities to misappropriate the University's assets.

At this stage, the University should decide if external parties including the funding body and the Police are to be involved. Delays in contacting the Police may prejudice future enquiries and alerting them immediately is important since they will be able to advise the University on how best to proceed and the most effective methods to gather evidence.

#### **2.5. Conducting a Fraud Enquiry**

Once it is agreed that there is sufficient evidence to justify a fuller investigation, the Fraud Investigation Group should meet with the Police, where appropriate, to decide who is best placed to undertake the further investigation. Should it be decided that an internal investigation is appropriate, either in tandem with a Police investigation, or on its own, it is important that it is undertaken by individuals with experience in fraud investigations. This may be the Internal Auditors, supported as necessary by

University staff who may have the specialist knowledge required. The decision by the group shall constitute authority to internal audit to use time provided in the internal audit plan for special investigations, or contingency time, or to switch internal audit resources from planned audits

Where fraud and corruption are suspected, contact by the Chief Financial Officer and the internal audit manager with the local fraud squad should be considered in order to agree an appropriate course of action.

For internal investigations, the Fraud Investigation Group should agree the following:

- detailed remit and scope for the investigation; for example, is it to confirm that there is sufficient evidence to support the allegations, to gather evidence for the Police, or does the University wish to quantify the total potential loss?
- who should undertake the investigation
- reporting procedures and deadlines
- a programme of regular meetings.

There is a clear requirement to record all details fully, accurately and in a manner that is accessible. The Police should be able to advise on an appropriate recording format. Developing a simple form to log all events and contacts made will provide a quick summary, ease the recording process and provide documented support for any future enquiries or possible prosecution.

## **2.6. Recovery of Losses**

It is important that any losses incurred by the University are fully and accurately recorded and that costs are correctly apportioned. In addition to the direct cost of losses attributable to fraud, all costs associated with enquiries should be recorded. These will be required under loss reporting procedures and may also be required by the courts if the decision to prosecute is taken and in determining any assessment of costs or compensation and insurance recoveries.

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.

## **2.7. Staffing Issues**

The Director of People is on the Fraud Investigation Group as further investigations may have implications for employee rights and disciplinary repercussions. Human Resources have a role to play in ensuring confidentiality and protecting individuals who report fraud, and any operational and policy developments should include input from Human Resources.

Of crucial importance in any fraud investigation is the need to conduct enquiries within the parameters of relevant laws and regulations. Employees have statutory rights and, if infringed, the likely success of disciplinary action or prosecution is diminished. It is vital therefore that any interviews with members of staff who are alleged to have acted fraudulently are undertaken strictly in accordance with established procedures.

For significant cases, no interviews should progress without first seeking advice from Human Resources on the relevant procedures and rules to be followed.

## **2.8. Reporting During the Investigation**

The Fraud Investigation Group should provide a confidential report to the Chair of the Court, the Chair of the Audit Committee, the Principal and, if appropriate, the external audit partner. Should an allegation result in an investigation into any of these office holders, the Group will report to only those office holders not implicated or other nominated individuals as appropriate. Updates should be provided at least monthly, unless the report recipients request a lesser frequency. The scope of the report should include:

- quantification of losses
- progress with recovery action
- progress with disciplinary action
- progress with criminal action
- estimate of resources required to conclude the investigation
- actions taken to prevent and detect similar incidents

Any variation from the approved fraud response plan, together with reasons for the variation, should be reported promptly to the chairs of both the Court and the Audit Committee.

## **2.9. Concluding an Investigation**

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 reoccurrence.

On completion of a special investigation, a written report should be submitted to the Audit Committee for consideration and discussion containing:

- a description of the incident, including the value of any loss, the people involved, and the means of perpetrating the fraud
- the measures taken to prevent a recurrence
- any action needed to strengthen future responses to fraud, with a follow-up report on whether or not the actions have been taken.

This report will normally be prepared by the Fraud Investigation Group or Internal Audit.

## **2.10. References for Employees Disciplined or Prosecuted for Fraud**

Any request for a reference for a member of staff who has been disciplined or prosecuted for fraud should be referred to the Head of Human Resources. The Head of Human Resources should prepare any answer to a request for a reference having regard to employment law.

## Checklist for Line Managers

The following is a checklist of points for consideration following the reporting of an alleged fraud to management:

- Do not rush in – consider all options and plan the approach.
- Establish the facts without alerting anyone.
- Maintain confidentiality.
- Make an immediate note of everything reported. Confirm accuracy of the notes with whoever is reporting the details to ensure clear understanding.
- Take steps to minimise any immediate further losses.
- Secure any evidence.
- Inform the Chief Financial Officer or member of the Fraud Investigation Group.

## Checklist for the Fraud Investigation Group

The following is a checklist of points for consideration following the reporting of an alleged fraud by line management to a member of the Fraud Investigation Group:

- Convene a meeting of the Group to consider the allegation.
- Conduct an initial investigation to establish the substance of the allegation.
- Consider legal implications.
- If substantiated, inform the Principal etc.
- Agree if further investigation is required and who will undertake it.
- Agree a remit and establish scope and reporting deadlines for the investigation.
- Ensure the investigating team has adequate resources, including secure storage.
- Prepare for interviews thoroughly.
- Ensure existing [staff disciplinary procedures](#) are followed.
- Secure any evidence.
- Assume the worst-case scenario in terms of losses and staff involved.
- If not already requested to undertake the investigation, inform the Police and the funding body as appropriate.
- Hold regular progress meetings at which progress and agreed action are documented.
- Identify all internal and external sources of information and evidence.