Southern Regional College

ANTI-FRAUD: POLICY AND PROCEDURE

Process Area	**Finance**
Reference Number	**FIN/007**
Directorate	**Finance and Planning**

Issue No	Date	Details	Author	Approved
001	Feb 2008	First Issue	TMcC	BD
002	Feb 2012	Change of Title from “Fraud” to “Anti-Fraud” Minor changes to all sections	JO’H	SMT / Audit Committee
003	Jan 2013	Reviewed - no changes made	JO’H	SMT / Audit Committee
004	Nov 2015	Reviewed – minor changes	JO’H	SMT / Audit Committee
005	April 2016	Reviewed to take account of DEL comments	JO’H	Governing Body
006	Aug 2017	Reviewed - SRC Logo updated no substantive changes	JO’H	SMT / Audit Committee
007	Aug 2018	Reviewed – minor changes	JMG/TMG	SMT / Audit Committee
008	Aug 2019	Reviewed – minor changes	JMG/TMG	SMT / Audit Committee
009	June 2020	Reviewed – minor changes agreed by Audit Committee	TMG	SMT / Audit Committee
010	Aug 2021	Reviewed – Direction update in absence of Director	JMG	Governing Body
011	Feb 2022	Section 4.11 update to Fraud Risk Assessments	JMG, LC	Governing Body
012	May 2023	Reviewed to add clarity around roles and responsibilities and improve the understanding of readers	LC	Governing Body
013	Apr 2024	Reviewed - no changes made	JMG	Governing Body

If requested, the College will make the policy available in alternative formats to accommodate visual impairments. The policy can also be downloaded from the College website and made available in alternative languages upon request.

1. POLICY STATEMENT

Southern Regional College (the College) requires all staff at all times to act honestly and with integrity and to safeguard the public resources for which they are responsible. Fraud is an ever-present threat to these resources and hence must be a concern to all members of staff.

The College takes a **zero-tolerance** approach to fraud. Cases will be thoroughly investigated, reported to the police as necessary, and appropriate action will be taken to recover monies lost as a result of fraud perpetrated against the organisation. The College is committed to ensuring that opportunities for fraud and bribery are minimised.

The procedures to be followed in the event of a fraud being detected or suspected are detailed in the College's Fraud Response Plan.

2. POLICY OBJECTIVE

There is a continuing need to raise staff awareness of their responsibility to safeguard public resources against the risk of fraud. The overall purpose of this policy, therefore, is to detail the relevant roles and responsibilities regarding the prevention, detection and response to fraud. The principles of this policy are based on Departmental guidance and on guidance issued by NIAO.

The purpose of this policy statement is to:

- provide a definition of fraud, corruption and bribery;
- set out responsibilities for fraud prevention and detection;
- set out procedures for reporting suspected and proven cases of fraud;
- set out responsibilities for the investigation of suspected fraud and proven cases of fraud; and
- set out responsibilities for bribery prevention and detection.

3. POLICY SCOPE

Since persons outside as well as those inside the College can perpetrate a fraud, this policy shall apply to members of the public as well as members of the Governing Body and Staff.

4. DEFINITIONS

Fraud

Fraud is when someone obtains financial advantage or causes loss by implicit or explicit deception. It is generally used to describe such acts as deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts and collusion. It can be further defined as any course of action involving dishonesty, where any person by the use of deception makes a gain for himself/herself or another or causes loss to another.

The Fraud Act 2006 came into effect in 2007. The Act states that a person is guilty of fraud if someone is in breach of any of the following:

- **Fraud by false representation**, i.e. if someone dishonestly makes a false representation and intends by making the representation to make a gain for himself or another, or to cause loss to another or expose another to risk of loss.

- **Fraud by failing to disclose information**, i.e. if someone dishonestly fails to disclose to another person information which he is under a legal duty to disclose and intends, by means of abuse of that position, to make a gain for himself or another, or to cause loss to another or expose another to risk of loss.

- **Fraud by abuse of position**, i.e. if someone occupies a position in which he is expected to safeguard, or not to act against, the financial interests of another person, and he dishonestly abuses that position, and intends, by means of the abuse of that position, to make a gain for himself or another, or to cause loss to another or to expose another to a risk of loss.

The Act also creates three new offences to assist in the fight against fraud. These include obtaining services dishonestly; of possessing, making, and supplying articles for use in frauds; and fraudulent trading.

Fraud can also be defined in a wider sense within the College environment to include acts of wrongdoing that may not be prosecuted under the Fraud Act 2006 but may be subject to internal investigation. This may include but may not be limited to:

- Misrepresentation of financial or non-financial data for non-statutory reporting purposes.
- Data theft.
- Misappropriation of supplies or other College assets.
- Bribery and corruption.
- Deception and collusion.

Fraud can be perpetrated by persons outside as well as inside the organisation.

Categories of fraud that may be relevant to the College include but are not limited to:

- Misappropriation of cash.
- Expenses claim fraud.
- Purchasing and payment system fraud.
- False salary claims (contracts or additional hours and adjustments).
- Theft of equipment or consumables.
- False accounting.
- Suppression or concealment or exploitation of documents or records.
- Abuse of flexitime system or unauthorised absence.
- Misuse of computer/IT facilities.

Attempted Fraud

The Act further requires that the person committing the fraud must do so with the intention of making a gain or causing loss or risk of loss to another. The key factor to consider is the intention of the individual concerned, not whether a gain or loss has actually taken place and should be treated as seriously as actual fraud and should be managed and reported as actual fraud.

Computer Fraud

Computer fraud is defined by the Computer Misuse Act 1990. Computer fraud is where information technology (IT) equipment has been used to manipulate computer programs or data dishonestly (for example by altering or substituting records, destroying or suppressing records, duplicating or creating spurious records), or where the existence of an IT system was a material factor in the perpetration of fraud (i.e. where the fraud was unlikely to have occurred if there had been no IT system). Theft or fraudulent use of computer facilities, computer programs and the Internet is included in this definition.

Corruption

Corruption is the offering, giving, soliciting or acceptance of an inducement or reward, which may influence the actions taken by any member of the College.

Corruption is further defined in the Bribery Act 2010 as relating to any or every person who by him/herself, or in conjunction with any other person, corruptly solicit, receive or agree to receive, for themselves or any other person, any gift, loan, fee, reward or advantage, whatsoever as an inducement to, or reward for, or otherwise on account of any member, officer or steward of a public body. This type of illegal activity may take the form of bribery, extortion, embezzlement, theft, or other abuse of power to gain unfair or illegal advantage.

Types of corruption include, but are not limited to, abuse in the following areas:

- Influencing exam results.
- Tendering and awarding of contracts.
- Profiteering because of knowledge of confidential College information or disclosing such information to other persons.
- Pecuniary interests of members and employees.
- Acceptance of inappropriate hospitality.
- Unauthorised disposal of college assets.
- Settlement of contractors' finance accounts/claims.
- Appointment and reward of consultants.

Bribery

Government guidance defines 'bribery,' as giving a financial or other advantage to any person (this may, for example, include donation to charity) to encourage that person to perform functions or activities improperly or to reward that person for having already done so.

The Bribery Act 2010 modernises the law on bribery and came into force on 1 July 2011. The Act is concerned with bribery. Very generally, this is defined as giving someone a financial or other advantage to encourage that person to perform their functions or activities improperly or to reward that person for having already done so. This could cover seeking to influence a decision-maker by giving some kind of extra benefit to that decision maker rather than by what can legitimately be offered, for example, as part of a tender process. The College could also be liable to a charge of bribery where someone who performs services on its behalf, for example an employee or agent, pays a bribe to get business, keep business, or gain a business advantage.

The Act details four main bribery offences: Bribing another person - offer, promise or give a financial or other advantage by intending to bring about improper performance. Being bribed - requesting, agreeing to receive, or accepting a bribe. Bribing a public official, including a foreign official - with intention of influencing the official in the performance of his/her official functions. Failure of a commercial organisation to prevent bribery by associated persons

The College will not tolerate bribery in any shape or form and will adopt a proportionate risk-based approach to ensuring adequate procedures exist and that staff are fully aware of and committed to the objective of preventing bribery.

The College will apply due diligence in the conduct of its business and will expect the same of those engaged on its behalf. The College will seek to ensure that bribery and fraud prevention is embedded in the organisation culture, processes, and procedures. Regular review of policies and procedures will take place and improvements made as appropriate.

5. ROLES & RESPONSIBILITIES

5.1 Chief Executive

The Chief Executive as Accounting Officer is responsible for establishing and maintaining a sound system of internal control that supports the achievement of College policies, aims and objectives. The system of internal control is designed to respond to and manage the full range of risks that the College faces. The system of internal control is based on an on-going process designed to identify the principal risks, to evaluate the nature and extent of those risks and to manage them effectively. The Orange Book: Management of Risk – Principles and Concepts contains guidance on identifying, assessing, and addressing risks.

Managing Fraud, Bribery and Corruption risk will be seen in the context of the management of this wider range of risks.

Although the Chief Executive bears overall responsibility and is liable to be called to account for specific failures, the Executive Team, Senior Management Team, all line managers and staff have a responsibility for acting to ensure that the College adopts an anti-fraud approach.

5.2 Director of Finance & Planning

The Director of Finance and Planning, as the Senior Responsible Officer, has overall responsibility for Fraud & Bribery Investigations, for managing the risk of Fraud and reporting any incidence. Their responsibilities include:

- Establishing an effective Anti-Fraud Policy and Fraud Response Plan.
- Establishing appropriate mechanisms for reporting Fraud Risk issues.
- Reporting all suspected incidents of Fraud to the Accounting Officer.
- External reporting all suspected incidents of Fraud as required.
- Liaising with the Audit & Risk Assurance Committee.
- Making sure that all staff are aware of the College’s Anti-Fraud Policy and know what their responsibilities are in relation to combating Fraud.
- Ensuring that vigorous and prompt investigations are carried out if Fraud occurs or is suspected.
- Taking appropriate action to recover assets.

5.3 Executive Team and Senior Management Team

It is the responsibility of the Executive Team and the Senior Management Team to support the Chief Executive by developing and maintaining effective controls to prevent fraud, bribery, and corruption and to ensure that if it does occur it will be detected promptly.

If Fraud occurs, Directors and Senior Managers must:

- Notify the Director of Finance & Planning, who in liaison with the Chief Executive will appoint an Investigating Officer.
- Co-operate with the Investigating Officer to ensure that a vigorous and prompt investigation is undertaken, which should consider as a matter of course whether there has been a failure of supervision.
- Ensure that the appropriate legal and/or disciplinary action is undertaken in all case where that would be justified.
- Make any necessary changes to systems and procedures to ensure that similar Frauds will not happen again.

In the absence of the Director of Finance and Planning all suspected or actual fraud must be reported directly to the Chief Executive.

5.4 Line Managers

Since line managers are responsible for ensuring that an adequate system of internal control exists within their areas of responsibility and that controls operate effectively, they are primarily responsible for the prevention and detection of Fraud, Bribery and Corruption.

Therefore, they must:

- Assess the types of risk involved in the operations for which they are responsible.
- Ensure that an adequate system of internal control exist within their area of responsibility.
- Regularly review and test the control systems for which they are responsible to ensure that controls are being complied with.
- Implementing new controls to reduce the risk where weaknesses have been identified.
- Satisfy themselves that their systems continue to operate effectively.

Internal Audit is available to offer advice and assistance on control issues, as necessary. In terms of establishing and maintaining effective controls it is generally desirable that:

- There is regular rotation of staff, particularly in key posts.
- Wherever possible, there is a separation of duties so that control of a key function is not vested in one individual.
- Backlogs are not allowed to accumulate.
- In designing any new system, consideration is given to building safeguards against internal and external fraud.

5.5 Staff Responsibilities

Every member of staff has a duty to ensure that public funds are safeguarded and therefore, **everyone is responsible** for:

- Acting with propriety in the use of College resources and the handling and use of College funds in all instances. This includes cash and/or payment systems, receipts and dealing with suppliers.
- Conducting themselves in accordance with the seven principles of public life detailed in the first report of the Nolan Committee ‘Standards in Public Life,’ i.e. selflessness, integrity, objectivity, accountability, openness, honesty, and leadership.

- Being vigilant to the possibility that unusual events or transactions could be indicators of fraud and alerting their line manager where they believe the opportunity for fraud exists. **Appendix 1** provides examples of Indicators of Fraud. In addition, Common Methods and Types of Fraud are included in **Appendix 2**, with examples of Good Management Practices, which may assist in combating fraud detailed in **Appendix 3**.

In addition, it is the **responsibility** of every member of staff, if they suspect that a fraud has been attempted or committed, or see any suspicious acts or events, to report details immediately to their line manager, Head of Faculty or Head of Functional Area who will be responsible for reporting the matter to the Director of Finance and Planning. (If there is concern that line management may be involved, the matter should be reported to the next appropriate level). The Public Interest Disclosure (NI) Order 1998 - Guidance on Public Interest Disclosure ('Whistleblowing') – protects the rights of staff who report wrongdoing. If you are in any doubt, you should speak to a senior officer, or the Director of Finance and Planning. The College **Public Interest Disclosure** (Whistleblowing) **Policy (PID) can** be found on the College Intranet together with the Public Interest Disclosure Response Plan Procedure.

Advice is also available through the independent charity Public Concern at Work on **020 7404 6609**. Their lawyers can give free confidential advice at any stage regarding a concern about serious malpractice at work. An employee can, of course, also seek advice from a lawyer of their own choice, at their own expense.

Section 5 of the Criminal Law Act (Northern Ireland) 1967 (Withholding Information) also places the onus on individuals to report/pass evidence to the Police. The involvement of the Police Service of Northern Ireland (PSNI) is dealt with in the **Fraud Response Plan.**

5.6 Internal Audit

Internal Audit is responsible for the provision of an independent and objective opinion to the Accounting Officer on risk management, control, and governance. The adequacy of arrangements for managing the risk of fraud and ensuring the College promotes an anti-fraud culture is a fundamental element in arriving at an overall opinion.

Internal Audit has no responsibility for the prevention or detection of fraud. However, internal auditors are alert in all their work to risks and exposures that could allow fraud. Individual audit assignments, therefore, are planned and prioritised to assist in deterring and preventing fraud by examining and evaluating the effectiveness of control commensurate with the extent of the potential exposure/risk.

Internal Audit is available to give advice on risk management/internal control issues and may, where necessary, provide advice in conducting fraud investigations.

5.7 External Audit

The role of the external auditor (the NI Audit Office) is to determine if the financial statements represent a "true and fair view" and that funds reported have been "applied to the purposes intended by the NI Assembly." In doing so the NIAO will obtain reasonable assurance that the financial statements taken as a whole are free from material misstatements, whether caused by fraud or error. If the auditor identifies a fraud or obtains information that indicates a fraud may exist, the auditors will communicate these matters to the appropriate level of management. It is for management to investigate such cases.

As with Internal Audit, it is not however the responsibility of external audit to prevent or detect cases of fraud. This is primarily a management responsibility.

5.8 The Audit and Risk Committee

The Audit & Risk Committee is responsible for understanding the College's strategy, control environment and risks, which includes an understanding of the College's fraud risk.

The Audit & Risk Committee is also responsible for:

- Understanding the role of those charged with governance in relation to managing risk (including fraud risk).
- Familiarisation with the college's policies and procedures relating to fraud risk.
- Understanding the college's framework and allocation of responsibilities for risk management.
- Being aware of the vulnerability of the college to changing conditions, such as economic pressures.
- Critically reviewing and challenging the framework for managing risk, including fraud risk.
- Critically reviewing and challenging the control environment in place to mitigate risk, including fraud risk.

5.9 DfE Fraud & Raising Concerns Branch

The Department for the Economy's Fraud and Raising Concerns Branch is also available to offer advice and assistance on risk management/internal control issues.

6. FRAUD RESPONSE PLAN AND FRAUD INVESTIGATION

The Southern Regional College has a Fraud Response Plan, which forms part of this Anti-Fraud Policy.

All staff should be alert to the possibility that unusual events or transactions can be symptoms of Fraud or attempted Fraud. Fraud may also be highlighted as a result of specific management checks or be brought to management's attention by a third party. It is College policy that there will be consistent handling of all suspected fraud cases without regard to position held or length of service, and investigators should have free access to all staff, records and premises in order to carry out investigations.

Any suspicions should be acted on promptly and all cases of suspected or actual fraud should be reported immediately to the appropriate line manager, Head of Faculty, Head of Functional Area, Assistant Director, or Director. If there is concern that the immediate Line Manager(s) may be involved, the matter should be reported to the next appropriate level. Additionally, management should immediately report the fraud or suspected fraud to the Director of Finance and Planning, the Director of Finance and Planning will inform the Chief Executive.

The Director of Finance and Planning will assess the matter and determine the appropriate action to be taken at this stage. The member of staff should not undertake preliminary enquiries until any suspicion has been reported to, and advice taken, from the Director of Finance and Planning.

Line managers should take care to ensure that any preliminary enquiries **do not prejudice subsequent investigations or corrupt evidence** and therefore should seek advice, as appropriate, at the earliest opportunity.

If an initial examination confirms the suspicion that a fraud has been perpetrated or attempted, management should follow the procedures provided in the College's **Fraud Response Plan**.

7. FRAUD RISK ASSESSMENTS

A major element of good corporate governance is a sound assessment of the organisation's business risks. The key to managing the risk of fraud is the same in principle as managing any other business risk and should be approached systematically at both the organisational and the operational level. The assessment of risk should be part of a continuous cycle rather than a one-off event: as systems and the environment change, so do the risks to which departments will be exposed.

CIPFA's Code of Practice1 states:

'Fraud risk identification is essential to understand specific exposures to risk, changing patterns in fraud and corruption threats and potential consequences to the organisation and its service users.'

Figure 1 below sets out the key stages of a risk management cycle to help deal with fraud. Internal Audit is available to offer advice and assistance on risk management/ internal control issues. In addition, **Appendix 4** provides Guidance on Performing an Assessment of Fraud Risks.

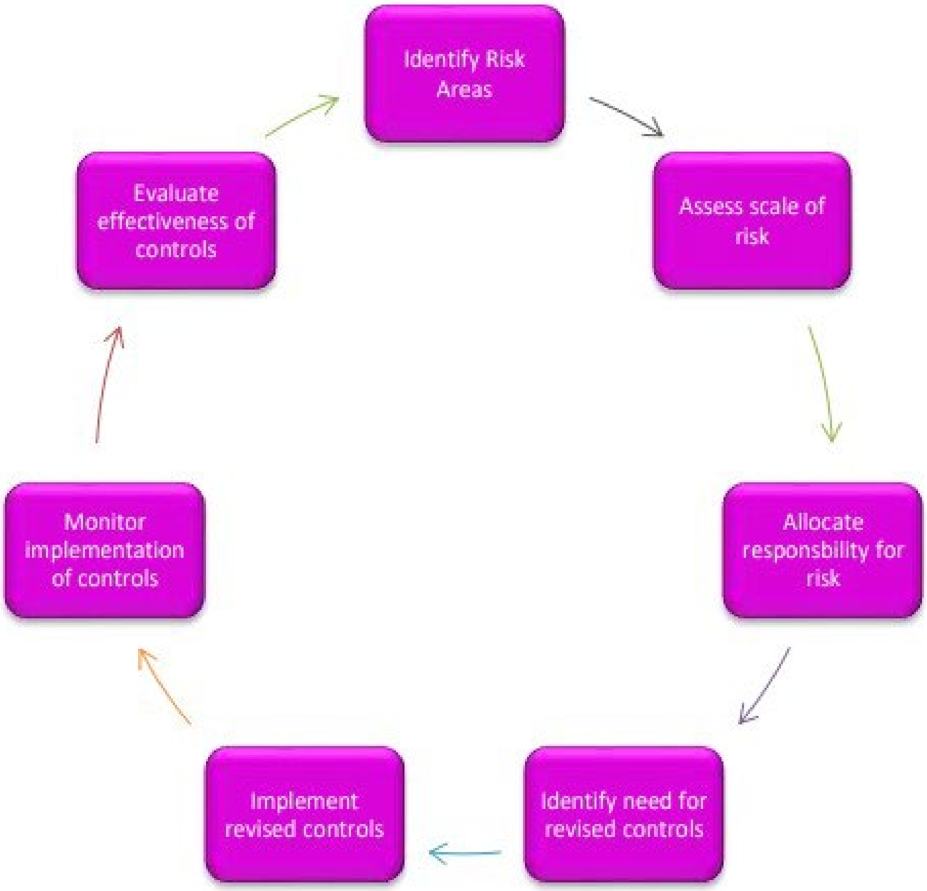
Identify Risk Areas
Assess scale of risk
Allocate responsbility for risk
Identify need for revised controls
Implement revised controls
Monitor implementation of controls
Evaluate effectiveness of controls

Figure 1: *Risk management cycle*

Fraud risk assessment should be reviewed every 2 years or when there is significant organisational change, to ensure that any new fraud risks are identified and addressed.

Fraud risk assessments should be reviewed by the Audit and Risk Committee.

Northern Ireland Finance Officers Network (NIFON) will share fraud risk assessments across the sector annually to ensure consistency and that any new risks are identified and considered.

8. NATIONAL FRAUD INITIATIVE (NFI)

The National Fraud Initiative (NFI) is a data matching exercise that compares information held by different organisations and within various parts of an organisation to identify potentially fraudulent claims and overpayments. The Comptroller and Auditor General for Northern Ireland can undertake data matching exercises, requesting data from a range of public bodies, for the purposes of assisting in the prevention and detection of fraud.

The College participates in the National Fraud Initiative liaising with other public authorities and bodies, providing data, and investigating matches that have been identified. The NFI represents another strand of the College's anti-fraud policy.

9. DISCIPLINARY ACTION

After full investigation, the College will take legal and/or disciplinary action in all cases where it is considered appropriate. Any member of staff found guilty of a criminal act will be considered to have committed a serious disciplinary offence and will be dismissed from the College on the grounds of gross misconduct.

Where supervisory negligence is found to be a contributory factor, disciplinary action may also be initiated against those managers/supervisors responsible.

It is College policy that in **all cases of fraud**, whether perpetrated or attempted by a member of staff or by external organisations or persons, the case will be referred, as appropriate, to the PSNI at the earliest possible juncture.

Appropriate steps will be taken to **recover all losses** resulting from fraud, if necessary, through civil action.

10. MALICIOUS OR VEXATIOUS REPORTS

If an allegation is made frivolously, in bad faith, maliciously or for personal gain, disciplinary action may be taken against the person making the allegation.

11. TRAINING

All new staff must complete mandatory Anti-Fraud Training, as part of their induction programme, the mandatory Anti-Fraud Training is refreshed on at least a tri-annual basis, and all staff will be required to complete any new releases of the training within 28 days of release.

In addition, Line Managers will review the need for refresher training for relevant staff, as part of the annual appraisal process. Where necessary refresher training will be included as part of individuals staff development programme.

12. DISTRIBUTION

- SharePoint
- All Clients

13. RELATED DOCUMENTS

- Fraud Response Plan
- Partnership Agreement between DfE and the College
- Fees Policy
- Annual Schedule of Fees & Charges
- Complaints and Compliments Policy
- Public Interest Disclosure (Whistleblowing) Policy
- Gifts and Hospitality Policy
- www.finance-ni.gov.uk/publications/anti-fraud-guidance
- Managing the Risk of Fraud (NI) - A Guide for Managers - December 2011 (finance-ni.gov.uk)
- Managing Fraud Risk in a Changing Environment A Good Practice Guide (NIAO, 2015)

14. FLOWCHART

Not applicable.

APPENDIX 1

INDICATORS OF FRAUD

- Missing expenditure vouchers and unavailable official records.
- Crisis management coupled with a pressured business climate.
- Profitability declining.
- Excessive variations to budgets or contracts.
- Refusals to produce files, minutes or other records.
- Related party transactions.
- Increased employee absences.
- Borrowing from fellow employees.
- An easily led personality.
- Covering up inefficiencies.
- Lack of board oversight.
- No supervision.
- Staff turnover is excessive.
- Figures, trends or results which do not accord with expectations.
- Bank reconciliations are not maintained or cannot be balanced.
- Excessive movement of cash funds.
- Multiple cash collection points.
- Remote locations.
- Unauthorised changes to systems or work practices.
- Employees with outside business interests or other jobs.
- Large outstanding bad or doubtful debts.
- Poor morale.
- Excessive control of all records by one officer.
- Poor security checking processes over staff being hired.
- Unusual working hours on a regular basis.
- Refusal to comply with normal rules and practices.
- Personal creditors appearing at the workplace.
- Non-taking of leave.
- Excessive overtime.
- Large backlogs in high risk areas.
- Lost assets.

Corporate Fraud

- Lack of thorough investigations of alleged wrongdoing.
- Pecuniary gain to organisation – but no personal gain

- Offices with excessively flamboyant characteristics.
- Employees suffering financial hardships.
- Placing undated/post-dated personal cheques in petty cash.
- Employees apparently living beyond their means.
- Heavy gambling debts.
- Signs of drinking or drug abuse problems.
- Conflicts of interest.
- Lowest tenders or quotes passed over with scant explanations recorded.
- Employees with an apparently excessive work situation for their position.
- Managers bypassing subordinates.
- Subordinates bypassing managers.
- Excessive generosity.
- Large sums of unclaimed money.
- Large sums held in petty cash.
- Lodgements not being cashed up on a timely basis.
- Lack of clear financial delegations.
- Secretiveness.
- Apparent personal problems.
- Marked character changes.
- Excessive ambition.
- Apparent lack of ambition.
- Unwarranted organisation structure.
- Absence of controls and audit trails.
- Socialising with clients – meals, drinks, holidays.
- Seeking work for clients.
- Favourable treatment of clients – e.g. Allocation of work.
- Altering contract specifications.
- Contract not completed to specification.
- Contractor paid for work not done.
- Grants not used for specified purpose – e.g. leasing capital equipment instead of purchasing them.

APPENDIX 2

COMMON METHODS AND TYPES OF FRAUD

- Payment for work not performed.
- Claiming for overtime not worked.
- Secondary employment during working hours.
- Abuse of flexi.
- Working while on sick leave.
- Over claiming travel and expenses.
- Running a private business with official assets, for example, departmental telephone and it systems.
- Forged endorsements.
- Altering amounts and details on documents.
- Collusive bidding.
- Overcharging.
- Writing off recoverable assets or debts.
- Unauthorised transactions.
- Selling information.
- Cheques made out to false persons.
- False persons on payroll.
- Theft of official purchasing authorities such as order books.
- Unrecorded transactions.
- Transactions (expenditure/ receipts/ deposits) recorded for incorrect sums.
- False official identification used.
- Damaging/destroying documentation.
- Using copies of records and receipts.
- Using imaging and desktop publishing technology to produce apparent original invoices.
- Charging incorrect amounts with amounts stolen.
- Transferring amounts between accounts frequently.
- Delayed terminations from payroll.
- Bribes.
- Skimming odd pence and rounding.
- Using facsimile signatures.
- False compensation and insurance claims.
- Stealing of discounts.
- Selling waste and scrap.
- Altering stock records.
- Altering sales records.
- Cash stolen.
- Supplies not recorded at all.
- Stolen equipment and supplies.
- Misuse of electronic signatures.

APPENDIX 3

EXAMPLES OF GOOD MANAGEMENT PRACTICES THAT MAY ASSIST IN COMBATING FRAUD

- Creation of a climate to promote ethical behaviour.
- All income is promptly entered in the accounting records with the immediate endorsement of all cheques.
- Regulations governing contracts and the supply of goods and services are properly enforced.
- Accounting records provide a reliable basis for the preparation of financial statements.
- Controls operate which ensure that errors and irregularities become apparent during the processing of accounting information.
- A strong internal audit presence.
- Management encourages sound working practices.
- All assets are properly recorded and provision is made known for expected losses.
- Accounting instructions and financial regulations are available to all staff and are kept up to date.
- Effective segregation of duties exists, particularly in financial accounting and cash/securities handling areas.
- Close relatives do not work together, particularly in financial, accounting and cash/securities handling areas.
- Act immediately on internal/external auditor’s report to rectify control weaknesses.
- Review, where possible, the financial risks of employees.
- Issue accounts payable promptly and follow-up any non-payments.
- Set standards of conduct for suppliers and contractors.
- Maintain effective security of physical assets; accountable documents (such as cheque books, order books); information, payment and purchasing systems.
- Review large and unusual payments.
- Perpetrators should be suspended from duties pending investigation.
- Proven perpetrators should be dismissed without a reference and prosecuted.
- Query mutilation of cheque stubs or cancelled cheques.
- Store cheque stubs in numerical order.
- Undertake test checks and institute confirmation procedures.
- Develop well defined procedures for reporting fraud, investigating fraud and dealing with perpetrators.
- Maintain good physical security of all premises.
- Randomly change security locks and rotate shifts at times (if feasible and economical).
- Conduct regular staff appraisals.
- Review work practices open to collusion or manipulation.
- Develop and routinely review and reset data processing controls.
- Regularly review accounting and administrative controls.
- Set achievable targets and budgets, and stringently review results.
- Ensure staff take regular leave.
- Rotate staff.
- Ensure all expenditure is authorised.
- Conduct periodic analytical reviews to highlight variations to norms.
- Take swift and decisive action on all fraud situations.
- Ensure staff are fully aware of their rights and obligations in all matters concerned with fraud.

APPENDIX 4

GUIDANCE ON PERFORMING AN ASSESSMENT OF FRAUD RISKS

This appendix provides guidance on how to perform an assessment of fraud risks using the template provided below.

Faculty/Business Area:	*[Insert name of faculty or business area]*
Fraud Risk Assessment of:	*[Insert a description of the area being assessed e.g. branch, process, type and value of transactions, nature of expenditure, any risks realised, any internal audit or external audit recommendations or concerns.*
Assessment completed by:	*[Insert name of officer completing the assessment]*
Assessment reviewed and agreed by:	*[Insert name of line manager reviewing and agreeing the assessment]*
Assessment agreed on:	*[Insert date assessment is agreed]*
Next assessment due on:	*[Insert date for completion of next fraud assessment]*

1	**2**	**3**	**4**	**5**	**6**	**7**
FRAUD RISK	**IMPACT (H, M, L)**	**LIKELIHOOD (H, M, L)**	**KEY CONTROLS**	**RESIDUAL RISKS**	**PLANNED ACTION**	**ACTION TAKEN**

How to complete the assessment

1. Identify the key fraud risks facing your business and detail these in **Column 1**.

   Examples might be:
   - fraudulent subsidy/grant claims;
   - payment made on false documentation;
   - theft of assets;
   - misappropriation of cash;

- false accounting;
- contract fraud;
- procurement fraud;
- collusion;
- computer fraud;
- fraudulent encashment of payable instruments;
- travel and subsistence fraud;
- false claims for hours worked; and
- bribery.

2. Assess the impact of the identified fraud risk should it occur – High, Medium or Low (**Column 2**). What damage could be done in relation to achievement of objectives, financial loss, reputation etc.?

3. Assess the likelihood of the identified fraud risk occurring – High, Medium or Low (**Column 3**). High would be probable/likely, low would be improbable/unlikely.

4. Identify the key controls already in place to address each identified risk (**Column 4**).

Examples might be:

- segregation of duties;
- payment authorisation levels;
- payment/lodgement reconciliations;
- management checks and reviews;
- tendering process;
- transparent approval process;
- inter-system checks;
- physical controls such as safes, key safes etc.;
- logical access controls;
- physical access controls;
- asset register and inventory checks;
- audit logs;
- project monitoring;
- performance monitoring;
- independent/unannounced inspections;
- post-payment checks;
- training;
- manuals;
- staff rotation;
- irregularity recording, investigation and reporting process etc.

5. Determine if any risk still exists after the application of the identified controls (**Column 5**). For example, the original risk detailed in column 1 will probably still be a risk post-control although the effective application of the controls detailed in column 4 will reduce the likelihood of occurrence.

6. Detail in **Column 6** what further action you are going to take to address the residual risk. It may be that control over the risk lies elsewhere and as a consequence you will have to accept the risk. If this is the case, justify why you are accepting the risk.

7. If you are planning further action to treat the risk, state what this is, who will be responsible for the action and when it is to be implemented.

8. **Column 7** will be used by you for internal reviews of the risk management framework.

9. Issue completed framework to the Head of Internal Audit annually. Review internally on a regular basis – at least every 6 months.