



SOUTH WEST GAUTENG TECHNICAL AND VOCATIONAL  
EDUCATION AND TRAINING COLLEGE  
EDUCATION OF DISTINCTION

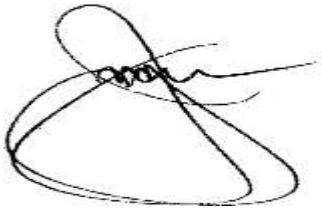

# **Quality Management System**

# **Policy on Fraud Risk Management**

This Policy on Fraud Risk Management has been issued on the authority of the College Council of South West Gauteng TVET College

**AMENDMENT AND APPROVAL RECORD**

| <b>Revision No.</b> | <b>Amendment description</b> | <b>Originator</b>       | <b>Approved By</b> | <b>Date</b> |
|---------------------|------------------------------|-------------------------|--------------------|-------------|
| 1.                  | New Policy of the College    | Policy Review Committee | Finance Committee  | .....       |

|  |   |  |
|--|---|--|
| <b>Policy on Fraud Risk Management</b>   |   |  |
| <b>Department: Finance</b><br><b>Responsibility : Accounting Officer</b>   |   |  |
| <p>Prepared and submitted by<br/>the Accounting Officer to<br/>Council</p>  <p>Date: 08 December 2021</p> | <p>Adopted by Council(Signed<br/>by Chairperson obo Council)</p>  <p>Date: 08 December 2021</p> | <p>Implementation</p> <p>Date:08 December 2021</p> |

|     | <b>TABLE OF CONTENTS</b>                                      | <b>PAGE</b> |
|-----|---|-------------|
| 1.  | <b>Background Information</b>                                 | <b>3</b>    |
| 2.  | <b>Legislative framework and best practice</b>                | <b>3</b>    |
| 3.  | <b>Purpose and Scope</b>                                      | <b>3</b>    |
| 4.  | <b>Definitions, acronyms, and abbreviations</b>               | <b>5</b>    |
| 5.  | <b>Actions Constituting Fraud</b>                             | <b>6</b>    |
| 6.  | <b>Understanding Fraud</b>                                    | <b>6</b>    |
| 7.  | <b>Regulatory Framework on Fraud and Corruption</b>           | <b>6</b>    |
| 8.  | <b>Governance Structures to manage Fraud &amp; Corruption</b> | <b>11</b>   |
| 9.  | <b>Overview of Fraud Risk Management</b>                      | <b>10</b>   |
| 10. | <b>Fraud Detection Strategies</b>                             | <b>21</b>   |
| 11. | <b>Response Strategies</b>                                    | <b>22</b>   |
| 12. | <b>Updating the Fraud Risk Management Policy</b>              | <b>24</b>   |
| 13. | <b>Adoption of policy</b>                                     | <b>24</b>   |
| 14. | <b>Availability of this policy</b>                            | <b>24</b>   |

## **1. BACKGROUND INFORMATION**

The provisions of Section 38(1)(a)(i) of the Public Finance Management Act stipulates that the Accounting officer/Authority is responsible for ensuring that the department , trading entity or constitutional institution has and maintains effective, efficient and transparent systems of financial and risk management and internal control. In the context of TVET Colleges, this is reinforced by Section 25(1) of the CET Act of 2006- (as amended) which requires Colleges to implement a risk management system no less effective than that prescribed to other state entities in the PFMA

Furthermore, sections 3.2.1 and 27.2.1 of Treasury Regulations require that a risk management is conducted on a regular basis and a risk management strategy, which includes a fraud prevention plan, be used to direct internal audit effort . The strategy must be clearly communicated to all employees to ensure that risk management including the College's approach to the prevention of fraud and corruption , is incorporated into the language and culture of the College.

## **2. LEGISLATIVE FRAMEWORK AND BEST PRACTISES**

Key principles contained in the following legislation were applied to develop this plan:

- a) Public Finance Management Act, 1999 (as amended )
- b) Continuing Education and Training Act No 16 of 2006 (as amended) (the Act)
- c) National Treasury regulations of March 2005 (as amended):
- d) National Treasury Public Sector Risk Framework, April 2010,
- e) The King Code of Governance Principles (King III).
- f) Prevention and Combating of Corrupt Activities Act No 12 of 2004,
- g) Public Sector Integrity Management Framework , and
- h) Code of Conduct for Public Servants in National and Provincial Departments ( Chapter 2 of Public Service Regulations, 2001, as amended)

The following College policies have a bearing on this policy:

- a) Risk Management Policy
- b) Whistle Blowing Policy
- c) Supply Chain Management Policy
- d) Recruitment and Selection Policy
- e) Employee Code of Conduct

## **3. PURPOSE AND SCOPE**

The purpose of the Fraud Risk Management Policy is to document the procedures in the event of reported or suspected fraud or irregularity, together with defining authority levels, responsibilities for action, and reporting lines. The objective is to safeguard the proper use of the Colleges finances and resources, and to protect the College reputation.

The Fraud Risk Management Policy applies to all Council members, all employees, contractors, vendors/suppliers, and any other party conducting business with the College. Any fraudulent or corrupt behaviour must be reported immediately through the mechanisms, as set out in this document and such reports will be investigated and acted upon.

#### 4. DEFINITIONS, ACRONYMS AND ABBREVIATIONS

For the purpose of this policy, unless the context indicates otherwise, the following definitions, acronyms and abbreviations are set out for the terms indicated:

- 4.1 **“Accounting Officer”** – is the College Principal.
- 4.2 **“Act”** – is the CET Colleges Act No.16 of 2006, as amended (formerly the FET Act)
- 4.3 **“Audit Committee” – “Audit Com”** – is the College Audit Committee.
- 4.4 **“Audit and Risk Management Committee”** – the committee per 4.3, combined with the “Risk Management Committee” (4.17) in order to streamline the governance process.
- 4.5 **“CET”**- is Continuing Education and Training.
- 4.6 **“College”** – is a Public TVET College (formerly known as a FET College).
- 4.7 **“Department”; “DHET”** – is the Department of Higher Education and Training.
- 4.8 **“Employee”** – is any official, employed by the College, or Department, irrespective of grade, full-time or part-time, or basis of remuneration: whether it be monthly, weekly, daily or on an hourly basis.
- 4.9 **“HR”** – Human Resources
- 4.10 **“Internal Auditing”** – is an independent, objective assurance and consulting activity designed to add value and improve a College’s operations. It helps a College accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of Risk Management, control, and governance processes.
- 4.11 **“Minister”** – is the Minister of the Department of Higher Education and Training.
- 4.12 **“Management Team”** – is the broad management team (BMT) of the College
- 4.13 **“TVET”** – is Technical and Vocational Education and Training.
- 4.14 **“VCET”** – is Vocational and Continuing Education and Training.
- 4.15 **“PFMA”** – is Public Finance Management Act (Act No. 1 of 1999 as amended by Act No. 29 of 1999).
- 4.16 **“PRECCA”**- is Prevention and Combating of Corrupt Activities Act 12 of 2004
- 4.17 **“POCA”** – is Prevention of Organised Crime Act 121 of 1996
- 4.18 **“Risk Management”** – is a systematic and formalised process to identify, assess, manage, and monitor risks.

4.19 **“Risk Management Committee”** – is the body through which the Audit Committee, appointed by Council, drives, and reviews the College’s system of risk management. To streamline the governance process and for improved cost efficiency, the Risk Management Committee is effectively combined with the Audit Committee (6.4), under one chairperson until College charters have been revised to give effect to this structure.

4.20 **“SWGC”** – South West Gauteng TVET College

## **5. ACTIONS CONSTITUTING FRAUD**

Actions constituting fraud refer to, but are not limited to:

- (a) Any dishonest, fraudulent, or corrupt act,
- (b) Theft of funds, supplies or other assets,
- (c) Maladministration or financial misconduct in handling or reporting of money, financial transactions, or other assets,
- (d) Making a profit from insider knowledge,
- (e) Disclosing confidential or proprietary information to outside parties for financial or other advantage,
- (f) Irregular destruction, removal or abuse of records and equipment,
- (g) Deliberately omitting or refusing to report or act upon report of any such irregular or dishonest conduct,
- (h) Bribery, blackmail, secret commissions and or extortion involving a College employee in the performance of her or his duties,
- (i) Abuse of education facilities,
- (j) Theft of time, and
- (k) Any similar or related irregularity,

## **6. UNDERSTANDING FRAUD**

To understand initiatives for managing fraud, theft, and corruption, one has to understand, what is meant by and what constitute fraud, theft, and corruption.

### **6.1 FRAUD**

#### **6.1.1 Definition of Fraud**

In South Africa, the common law offence of fraud is defined as “the unlawful and intentional making of a misrepresentation which causes actual prejudice, or which is potential prejudicial to another”. The term “fraud” is also used in a wider sense by the general public. In this document, the term is used in its widest possible sense and is intended to include all aspects of economic crime and acts of dishonesty (including the legal definitions of fraud, theft, and

corruption). Fraud can also be described as any conduct or behaviour of which a dishonest representation and/or misappropriation forms an element.

### 6.1.2 Forms of Fraud

Fraud can be perpetrated in the following ways:

- (a) **By Management:** This is fraud involving one or more of the Council members or members of management of SWGC using their position of influence. Fraud by management may include collusion with third parties outside the entity.
- (b) **By Employees:** This is fraud involving employees of SWGC and may include collusion with third parties outside the entity.
- (c) **Fraudulent Reporting:** Fraudulent reporting involves intentional misstatements or omissions of amounts or disclosures in reports in order to deceive the users of the reports.

## 6.2 CORRUPTION

### 6.2.1 Definition of Corruption

Corruption in its wider meaning, and as referred to in this document, includes any conduct or behaviour where a person accepts, agrees, or offers any gratification for him/her or for another person where the purpose is to act dishonestly or illegally. Such behaviour also includes the use of material or information, abuse of position of authority or a breach of trust or violation of duty.

### 6.2.2 Forms of Corruption

Corruption takes various forms in society; the following are examples of different types of corruption:

- a) Manipulating a tender process to achieve a desired outcome.
- b) Misusing or disclosing official information
- c) Certifying the supply of goods or performance of services, without being certain, that the goods/services were really delivered/provided.
- d) Favours an applicant for employment on criteria, other than merit and the applicable policies relating to Employment Equity
- e) Allowing a conflict of interest to undermine one's independence; and
- f) Extracting money from students or parents for assumed registration preference

These manifestations are by no means exhaustive as corruption appears in many forms and it is virtually impossible to list all of these.

### 6.3 THEFT

A person commits the Common Law offence of **theft** if they “unlawfully appropriate of movable corporeal property belonging to another with intent to deprive the owner permanently of the property”.

## 7. REGULATORY FRAMEWORK RELEVANT TO FRAUD AND CORRUPTION

The following legislation stipulates the relevance of fraud, corruption and misconduct and provides the regulatory basis for the fraud prevention plan.

### 7.1 PREVENTION AND COMBATING OF CORRUPT ACTIVITIES ACT, 12 OF 2004

The Prevention and Combating of Corrupt Activities Act (generally referred to as “PRECCA”) is aimed at the strengthening of measures to prevent and combat corrupt activities.

PRECCA refers to a wide range of offences relating to corrupt activities. The offences defined by PRECCA refers to a giving or receiving a “gratification”. The term gratification is defined in PRECCA and includes a wide variety of tangible and intangible benefits such as money, gifts, status, employment, release of obligation, granting of rights or privileges, and the granting of any valuable consideration such as discounts etc.

#### 7.1.1 Offences under the PRECCA

A general description of corruption is contained in Section 3 of the PRECCA. This section provides that any person who gives or accepts or agrees or offers to accept/receive any gratification from another person in order to influence such other person in a manner that amounts to:

- The illegal or unauthorized performance of such other person’s powers, duties, or functions
- An abuse of authority, a breach of trust, or the violation of a legal duty, or a set of rules
- The achievement of an unjustified result
- Any other unauthorized or improper inducement to do or not to do anything is guilty of the offence of Corruption.

#### 7.1.2 Reporting of offences

**Section 34** of PRECCA places a duty on any person in a position of authority to report suspected corrupt or illegal activities to any police official. These activities include offences of corruption as defined under the PRECCA, as well as fraud, theft, extortion, and forgery, where the amount involved exceeds R100 000.

“Position of authority” is defined in the Act and includes wide range of persons in authority both public and private entities.

Failure to report such suspicions constitutes an offence.



### **7.1.3 Penalties**

Offences under the Act are subject to penalties including imprisonment for life and fines of up to R250 000. In addition, a fine amounting to five times the value of the gratification involved in the offence may be imposed.

## **7.2 PREVENTION OF ORGANISED ACT, 121 OF 1998**

The Prevention of Organised Crime Act as amended (generally referred to as “POCA”) relates to the provisions that aimed at preventing and combating of organised crime, money laundering and criminal gang activities.

POCA contains provisions that are aimed at achieving inter alia the following objectives

- a) The combating of organised crime, money laundering and criminal gang activities.
- b) The criminalisation of conduct referred to as “racketeering”.
- c) The provision of mechanisms for the confiscation and forfeiture of the proceeds of crime.
- d) The creation of the mechanisms for the National Director of Public Prosecutions to obtain certain information required for purposes of an investigation, and
- e) The creation of mechanisms for co-operation between investigators and the South African Revenue Services (SARS).

**Section 4** of POCA defines the “general” of money laundering and provides that a person who knows, or ought reasonably to have known, that property is, or forms part of the proceeds of unlawful activities, commits an offence if he commits an act in connection with that property which has the effect or is likely to have the effect of concealing the nature and source thereof.

**Section 5** of POCA stipulates that it is an offence if a person knows or ought reasonably to have known that another person has obtained the proceeds of unlawful activities and aids such other person regarding the use or retention of such proceeds.

**Section 6** of the POCA stipulates that it is an offence if a person knows or ought reasonably to have known that property is or forms part of the proceeds of unlawful activities and acquires uses or possesses such property.

The above offences are regarded as serious and the Act contains harsh penalties relating to these offences. A person convicted of one of the above offences is liable to a maximum fine of R100 million or to imprisonment for a period not exceeding 30 years.

## **7.3 PROTECTED DISCLOSURES ACT, 26 OF 2000**

The Protected Disclosure Act was promulgated to facilitate reporting by employees (whistle blowers) of fraud, corruption or other unlawful or irregular actions by the employer (s) or co-employees without fear of any discrimination or reprisal by their employer (s) or co-employees.

An employee who has information of fraud, corruption or other unlawful or irregular action (s) by his/her employer (s) or co-employees can report such actions, provided that he/she has evidence that:

- 7.3.1** A crime has been, is being or likely to be committed by the employer or employee (s)
- a) The employer or employees has/have failed to comply with an obligation imposed by law.
  - b) A miscarriage of justice has or is likely to occur because of the employer's or employee (s) actions.
  - c) The health or safety of an individual has been, is being, or is likely to be endangered.
  - d) The environment has been, is being, or is likely to be endangered.
  - e) Unfair discrimination has been or is being practiced; and
  - f) Any of the above has been, is being, or is likely to be concealed.

**7.3.2** As long as the disclosure is made in terms of the Protected Disclosure Act, the employer is prohibited from:

- a) Dismissing, suspending, demoting, harassing, or intimidating the employee.
- b) Subjecting the employee to disciplinary action.
- c) Transferring the employee against his or her will.
- d) Refusing due transfer or promotion.
- e) Altering the employment conditions of the employee unilaterally.
- f) Refusing the employee, a reference or providing him/her with an adverse reference.
- g) Denying appointment.
- h) Threatening the employee with any of the above; and
- i) Otherwise affecting the employee negatively.

#### **7.4 PUBLIC FINANCE MANAGEMENT ACT, 1 OF 1999**

The Act relates to the regulation of financial management in government and provincial governments. It is to ensure that all revenue expenditure, assets, and liabilities of those governments are managed efficiently and effectively. It is to provide for the responsibilities of persons entrusted with financial management in those governments and to provide for matters connected.

**Section 38 and 50** of the PFMA sets out the responsibilities of constitutional institutions and for accounting authorities and officials of public entities in that they must ensure that the organisation concerned has and maintains an:

- Effective, efficient, and transparent systems of financial and risk management and internal control.
- Prevent unauthorised; irregular and fruitless and wasteful expenditure and losses resulting from criminal conduct

**Section 38 (g)** provides that the accounting officer must on discovery of any unauthorised, irregular or fruitless and wasteful expenditure, immediately report, in writing particulars of the expenditure to the relevant treasury and in the case of irregular expenditure involving procurement of goods or services, also to the relevant tender board.

**Section 38 (h)** provides that the accounting officer must take effective and appropriate disciplinary steps against any official in the service of the department, trading entity or constitutional institution who:

- Contravenes or fail to comply with the provisions of the Act.

- Commits an act which undermines the financial management and internal control system of the department, trading entity or constitutional institution; or
- Makes or permits an unauthorised expenditure, irregular expenditure, or fruitless and wasteful expenditure.

**Section 40 (3) (b)** provides that the annual report and audited financial statements must include particulars of:

- Any material losses through criminal conduct, and any unauthorised expenditure, irregular expenditure, and fruitless and wasteful expenditure, that occurred during the financial year.
- Any criminal or disciplinary steps taken as a result of such losses, unauthorised expenditure, irregular expenditure, and fruitless and wasteful expenditure.

SWGCG's management adheres to principles of good corporate governance and also the PFMA. These entail planning of projects in a manner that will ensure:

- Irregular, fruitless and wasteful expenditure is minimised or avoided.
- Potential problems that might delay completion of the project are identified and properly managed.
- Project budgeted costs are adhered to; and
- Projects are completed promptly.

The planning should include the following:

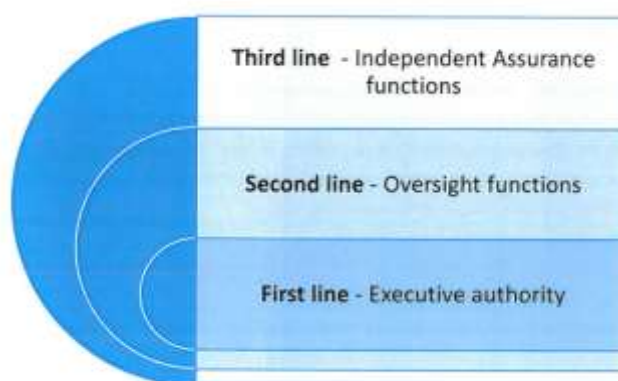
- The estimated costs of the projects.
- The resource requirement of the projects, and
- The required completion date of each significant phase

Project implementation managers should exercise due diligence and care in the following:

- Project delivery reports to assess deliverables,
- Ensure prompt and detailed follow up of vacancies,
- Time sheets and expense claims before authorising payment,

## 8. GOVERNANCE STRUCTURES TO MANAGE FRAUD AND PREVENTION

SWGCG is committed to the highest standards of Corporate Governance, including fraud risk management. SWGCG's Governance framework for managing fraud contains three lines of defence which are set out below:



### **8.1 First layer of responsibility - Executive Authority**

The College Broad Management Team takes an interest in fraud risk management to the extent necessary to obtain comfort that properly established and functioning systems of risk management are in place to protect the College against significant fraud risks.

The Executive Authority is responsible for the following:

- Treating fraud as a strategic risk and adopting a proactive strategy to mitigate the risk.
- Assuming the overall responsibility to ensure that external stakeholders and employees are protected from fraud,
- Ensure the establishment and enforcement of anti-fraud policies and procedures; and
- Mandate the operational responsibility for fraud risk management.

### **8.2 Second layer of responsibility – Oversight functions**

The oversight function includes an Audit and Risk Committee that has oversight of risk management. This committee is responsible to review the effectiveness of risk management specifically to:

- Ensure that SWGC has a clearly defined risk management strategy with appropriate supporting processes and structures.
- Review and assess the integrity of the risk management systems and ensure that the risk policies and strategies are effectively implemented.
- Formulate an independent and objective review of risk management within SWGC; and
- Adopt a holistic approach to risk management taking cognisance of financial, operational as well as fraud risk.

### **8.3 Third layer of responsibility – Independent assurance functions**

The role of the Internal Auditing in fraud risk management is to provide an independent, objective assurance on the effectiveness of the College's system of fraud risk management. Internal Auditing must evaluate the effectiveness of the entire system of fraud risk management and provide recommendations for improvement where necessary.

The internal audit function is responsible for the following:

- Providing an assessment of the effectiveness of SWGC's risk management and internal control framework.
- Devising an audit plan that identifies potential risks and devising strategies to overcome the risk.
- Evaluating and analysing business and governance processes.
- Providing a written assessment on the effectiveness of the system of financial controls to the Audit and Risk committee; and
- Providing a written assessment on the effectiveness of the system of internal controls and risk management to council.

## **9. OVERVIEW OF FRAUD RISK MANAGEMENT**

### **9.1 FRAUD TRIGGERS**

In order for fraud to occur there are normally three fraud triggers i.e. Opportunity, Motivation and Rationalisation.

**9.1.1 Opportunity** – refers to the perceived opportunity to perpetrate fraud against BBC e.g. a weak internal control management.

**9.1.2 Motivation** – refers to the perceived non-sharable need for committing the fraud e.g. personal debt burden.

**9.1.3 Rationalisation** – refers towards the frame of mind of the fraudster to justify his/her dishonest act.

### **9.2 MANAGING FRAUD**

A comprehensive approach to managing fraud, theft and corruption as explained above, includes three components, namely:

**9.2.1 Prevention** – preventing the occurrence of fraud

- a) Creating an ethical culture
- b) Ethics communication and training
- c) Fraud risk assessments
- d) Fraud awareness training
- e) Employee induction training
- f) Employee screening
- g) Vendor due diligence; and
- h) Conflict of internal checks

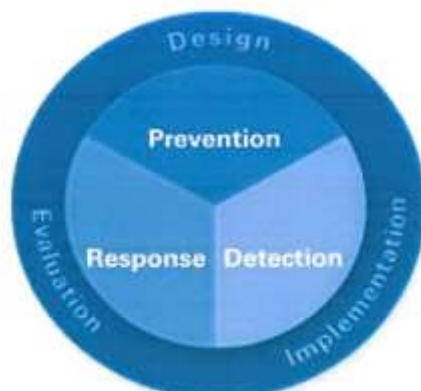
**9.2.2 Detection**- detecting existing instances of fraud'

- a) Surprise fraud audits.
- b) Post fraud control reviews.
- c) Whistleblowing facilities; and
- d) Forensic data analysis

**9.2.3 Response** – responding to the negative consequences of fraud

- a) Fraud response plan.
- b) Investigation
- c) Disciplinary Action
- d) Criminal prosecution; and
- e) Civil recovery

The graphic depiction below illustrates the above-mentioned better practice model while also taking cognisance of the perpetual cycle of design, implement and evaluation.



### **9.3 SWGC'S FRAUD PREVENTION INITIATIVES**

The prevention of fraud is reliant upon the design and implementation of formal strategies and procedures that minimize opportunities for fraud ("soft controls"), as well as the initiatives aimed at reducing the motivation for, and the realisation of fraud ("soft controls"). The initiatives below represent a combination of both hard and soft controls for the prevention fraud of SWGC.

#### **9.3.1 CODE OF ETHICS AND BUSINESS CONDUCT**

The Code provides a framework for identifying conduct that is ethical and acceptable for the employees of SWGC who effectively act as agents of all levels. The collective ethical conduct of all the individual employees if SWGC reflects SWGC's ethical conduct. In this regard, the highest standard of ethics is required from employees when fulfilling their duties.

Ethics training will be conducted at induction and on a continuing basis. The training will serve not only to highlight unethical and unacceptable business conduct and the resultant disciplinary action, but also to reiterate SWGC's shared core values of the impact these values have on employee's day-to-day operations.

The training will include an emphasis on:

- a) The importance of ethics within SWGC and the consequences (for individual employees, but also for SWGC as a whole) for unethical conduct.
- b) Identifying ethical dilemmas, and strategies for resolving ethical dilemmas.
- c) Understanding specific policies Within SWGC (i.e., on gifts or conflicts of interests).
- d) Mechanisms for reporting illegal and unethical conduct and the measures taken to protect whistle-blowers; and

- e) Ethics training will include awareness regarding SWGC's Whistle Blowing Policy and reporting channels.

### **9.3.2 FRAUD RISK ASSESSMENTS**

*"Hard controls"* for the fraud prevention are procedures designed to minimize opportunities to commit fraud. At SWGC, this includes fraud risk assessments, function-or process-specific fraud training, and the declaration of conflicts of interests, internal audit procedures and pre-employments screening.

Assessment of fraud risks

#### **Identifying locations or processes to assess**

The objective of this phase is to determine at what level to perform the assessment i.e., business unit level, business process level or transactional level or a combination of these. Consideration of which, locations of processes to assess might also be determined by the following:

- Prior fraud incidents.
- Critical processes; and
- Operations susceptible to fraud

#### **Identifying risk exposures**

The objective of this phase is to generate a register (the Fraud Risk Register) of all possible inherent risks for subsequent analysis. All inherent risks identified should be documented at this point regardless of whether a preliminary assessment concludes that internal controls currently in force will be fully effective in mitigating the risk. How each risk manifests itself should be documented as well as why it occurs.

#### **Analysing the risk exposures.**

All internal controls that are currently in force and which would tend to have the effect of mitigating the risk of fraud and corruption under consideration will be recorded. The effectiveness of all mitigating internal controls will be assessed. The assessment should conclude, in relation to each control, whether it is or likely to be:

- High
- Medium
- Low

In mitigating the risk to which it relates.

The assessment of each internal control considered should not be represent an assessment of the control in terms of its ability to mitigate business risk generally. Rather, it is an assessment of that control's perceived impact on the specific fraud or corruption risk under consideration.

### **Evaluating the risk exposures**

Each risk exposure will be evaluated i.e., high, medium, or low and this will allow SWGC to prioritise which risk exposure requires immediate action.

### **Implementing prevention plans**

All fraud and corruption risks rated at "Medium" and "High" will require the development and implementation of all proposed action aimed at achieving one or more of the following:

- Alteration to existing internal control procedures.
- Introducing new internal control procedures; and
- Introducing procedures aimed at detecting and preventing fraud.

Proposed action may also be developed in relation to risks assessed as being of a lower le residual risk. All actions proposed by the risk assessment team will be evaluated by senior management, as appropriate, prior to implementation.

The above will be formulated into a "Fraud Risk Register" which will prioritise the fraud and corruption risks and indicate actions to mitigate these risks.

Annually, management presents these revised risks with mitigating techniques to the Audit Committee for consideration. The risks that are both inadequately managed and carry material risk in the current environment are addressed as new systems are required.

The results of the fraud risk assessment will be documented in a Fraud Risk Register, which will be maintained by The Accounting Officer and form part of his/her report to the relevant risk committees.

### **9.3.3 EMPLOYEE FRAUD AWARENESS TRAINING**

In specific areas of SWGC's operations where it is deemed that a high residual risk of fraud, theft or corruption exists, appropriate fraud prevention training should be provided. For example, conducting due diligence on selected vendors or any other contracting parties.

In this regard, employees will receive training on the following:

- 1) Fraud prevention and strategy plan and employees' responsibilities to mitigate/reduce SWGC's risk due to fraud and misconduct:
- 2) Code of Conduct.



- 3) Procedures/channels available to employees to seek advice and report suspected misconduct:
- 4) Latest fraud trends:
- 5) Relevant regulatory requirements.
- 6) Manifestations of fraud and corruption in the workplace.
- 7) Information security - management of intellectual property and confidential information to limit the risk of manipulation of information:
- 8) How to report fraud and corruption.
- 9) The frequency of training and communication will be at induction, on an ongoing basis and as and when deemed necessary. Training will be provided in a variety of methods such as formal informal meetings, email correspondence etc.

### 9.3.4 PRE-EMPLOYMENT SCREENING

Pre-employment screening should be carried out and evidence of such screening maintained by the HR Department

SWGFC will ensure that the pre-employment screening procedures are applicable to all employees, regardless of level, including employees acting in specific positions, temporary and contract workers.

Limited procedures may be performed in the case of contract employees.

Screening will be conducted in accordance with the classification of the employees or the levels of screening outlined below:

| The following are the recommended checks that may be performed: |   |   |
|---|---|---|
| Level 1   | Contract Employees  | <ul style="list-style-type: none"> <li>• Education check</li> <li>• Previous Employment check</li> <li>• Reference Check</li> </ul>   |
| Level 2   | Non- Management Employees (who are not joining sensitive functions) | <ul style="list-style-type: none"> <li>• Education check</li> <li>• Previous Employment check</li> <li>• Reference Check</li> <li>• Criminal Record Check</li> </ul>  |
| Level 3   | Management Employees and employees are joining sensitive functions. | <ul style="list-style-type: none"> <li>• Education check</li> <li>• Previous Employment check</li> <li>• Reference Check</li> <li>• Criminal Record Check</li> <li>• Credit Check</li> <li>• Psychometric Checks</li> <li>• Directorship and Membership searches</li> </ul> |

SWGC procedures for pre-employment screening will also include all new management and employees promoted to management positions. The screening will be performed by a person/people nominated by the HR Department, to ensure that the screening is consistent and appropriately resourced throughout SWGC.

### **9.3.5 RECRUITMENT PROCEDURES**

The fight against fraud should start even before an employee is appointed. Employee focused fraud prevention measures will be visible from the point of advertising a vacant position, recruitment, specific employment conditions, maintaining high employee morale, performance management and even exit procedures upon resignation or retirement. SWGC will ensure that there is an inclusion of specific provisions when advertising posts to advise applicants that only people with the highest levels of personal integrity will be considered and that submission to appropriate pre-employment screening processes are obligatory for consideration in any post.

Recruitment will be conducted in accordance with the requisite recruitment procedures. It will be a transparent process and all appointments will be conformed only after due recommendation. Any person involved in any decision-making process, who may have a conflict of interest, must declare such a conflict in writing to the HR Department, and withdraw from any further procedures. Should it be subsequently identified that a person involved in the decision-making elements of the recruitment process has a relationship with the potential employee and, has not declared the potential conflict, may be subject to disciplinary procedures.

### **9.3.6 VENDOR DUE DELIGENCE PROCEDURES**

The following due diligence procedures will be considered:

Declarations- Declarations may be requested from the vendor regarding:

- Any potential conflict of interest due to the expected relationship: whether there exists any relationship between the vendor's employees and SWGC employees.
- Relationships between the vendor/vendor's, employees/vendor's, owners, and other vendors of SWGC:
- On an annual basis, declaration may be requested to be resubmitted by the vendors; and
- All such declarations may be reviewed to identify potential risks to SWGC.

### **9.4 CONFLICT OF INTERESTS**

A conflict of interest exists when an employee or other SWGC representative has a financial or other interest that could unduly influence his/her decision on the matter under consideration.

Furthermore, a conflict of interest exists when the objectivity of a person will be impaired by being part of the decision-making process on the matter, he/she has interest in.

SWGC will keep a register of employees' interest in suppliers and/or other entities and/or in specific SWGC contracts. Such employees should refrain from being involved in the decision-making process of the matter under consideration.

The declaration of the aforesaid conflict of interest does not permit the employees to enter into contracts they have interest in.

Failure to disclose actual or potential conflicts of interest by any party may result in disciplinary action against that party.

## 9.5 BLACKLISTING OF TRADING PARTNERS

The following criteria should be used to blacklist trading partners:

- (a) Non-performance on the previous contract with SWGC.
- (b) Cancellation of previous contracts with SWGC without valid reasons; and
- (c) Court judgments that are due to their dishonesty and lack of integrity in dealings with other parties.

The blacklisted trading partners should be listed in a register linked to SWGC service supplier database, i.e. National Treasury Central Supplier Database (CSD), and the register is checked annually to limit the risk of contracting with these suppliers again.

## 9.6 GIFTS AND ENTERTAINMENT

It is an established fact that employees face real challenges to their integrity in the form of enticement to accept bribes from unethical suppliers, contractors, consultants, etc. Furthermore, these trading partners are also sometimes untrustworthy in delivery of goods and/or services.

As per the College Code of Conduct, SCM officials and other role players must not:

- Seek or accept a bribe or other improper inducement:
- Seek gifts or benefits of any kind.
- Accept any gift or benefit that may create a sense of obligation or may be perceived to be intended or likely to influence the officials during the execution of public duty:
- Accept any gift or benefit of more than R350; and
- Accept an offer of money, regardless of the amount.

All gifts or benefits should be recorded in the gifts register. Any gifts or benefits received of more than R350 that cannot be reasonably refused or returned, must be disclosed to the Accounting Officer.

Gifts or benefits exceeding R350 must be surrendered to the College Accounting Officer, unless the nature of the gift or benefit makes this impractical. **The Accounting Officer must delegate the gift towards the overall benefit of the College, depending on the nature of the gift. Consideration for auction of the gift should be made, to dispose of the gift. Proceeds of the auction to be utilised towards the benefit of the College. The gift should be kept in a safe place until disposed.**

SCM officials must avoid situations giving rise to the appearance that a person or body, through the provision of gifts, benefits, or hospitality of any kind, is attempting to secure favourable treatment from the SCM Unit or the College Management.

A standard declaration form should be completed by all officials in relation to gifts, benefits, or hospitality of any kind, received/offered.

Employees shall not accept pay or give any form of bribe, kickbacks, and lavish gifts. SWGC representatives should not use their official position to obtain gifts or other gratuities.

The Accounting Officer must promptly report any alleged contravention as stated above to the National Treasury for considering whether the offending person, and any representative or intermediary through which such person is alleged to have acted, should be listed in the National Treasury's database of persons prohibited from doing business with the public sector.

This process does not apply to gifts less than R350 in value.

Failure to disclose gifts of a value greater than R350 shall be a disciplinary offence.

## **9.7 INFORMATION SECURITY**

SWGC encourages the use of IT in support of teaching and learning and to promote effective communication and working practices in furtherance of the College's mission.

Significant amounts of information are held in database and other format to aid communication within SWGC. If improperly managed, sensitive data could end up in the hands of unauthorized individuals.

Physical and logical access controls over the computer systems will continually seek to achieve the following:

- a) Striking the right balance between allowing access to information to enable efficient operations and denying inappropriate access to ensure that information is not compromised.
- b) Implementation of preventative controls to limit access to authorized persons; and
- c) Implementing detection controls to determine whether unauthorized access is being attempted or unusual patterns of activity are occurring.

SWGC will ensure that all employees are sensitized on a regular basis to the fraud risks associated with the information security and the utilization of computer resources, in particular access control, and ensure that controls are developed to limit the risk of manipulation of computerized data.

Regular communiques will be forwarded to employees pointing out security policies, with a particular emphasis on email and internet usage and the implications (e.g. disciplinary action) of abusing these and other computer related facilities. Where employees are found to have infringed on prevailing policy in this regard, disciplinary action will be taken.

Regular reviews of information and computer security will also be considered. Weaknesses identified during these reviews will be addressed.

## **10. FRAUD DETECTION STRATEGIES**

SWGC's aim is for the effective and swift detection of fraud that will ensure that prompt action is taken to minimize losses to SWGC.

Detection of fraud and corruption may occur through:

- Vigilance on the part of employees and executive management.
- The internal audit function, including surprise fraud audits.
- Anonymous whistle blowing reports; and
- The application of forensic data analytics technics.

SWGC will conduct random detection reviews, with due consideration for the use of automated tools in the following high fraud risk areas on a regular basis in order to pro-actively detect frauds:

- Procurement and tendering.
- Contracts management; and
- Project management and supervision.

### **INTERNAL AUDIT**

A robust internal audit programme serves as an effective preventative measure of detecting control deficiencies prior to fraud occurring. Internal audit will be responsible for implementing an internal audit programme which will incorporate steps to ensure adherence to internal controls to mitigate fraud and corruption.

The internal audit programme will also include a review of transactions after they have been processed and completed. This review can be effective in identifying fraudulent or corrupt activity. In addition to the possibility of detecting fraudulent transactions, such a strategy can also have a significant fraud prevention effect as the threat of detection maybe enough to deter a staff member who would otherwise be motivated to engage in fraud and corruption.

### **HOTLINE FOR REPORTING FRAUD**

A whistle blowing facility is one of the most effective tools in identifying current fraud occurring within an organization. One of these channels, which clearly enhance SWGC's detection capacity, is the fraud hotline. Employees and other parties are encouraged to report their suspicions of fraud without fear of reprisal.

The following general provisions apply to whistle-blowing facilities:

- All employees and suppliers can contact the hotline email to voice any concerns that they have relating to fraudulent behaviour at SWGC (Annexure A - Letter to Suppliers-Declaration 2021F).
- Trained operators will respond to emails in most of the official languages in South Africa.
- Our dedicated whistle blowing consultant(s) that will be responsible for monitoring emails sent to the hotline will probe whistle blowers for specific facts to record as much information and understand the incident as clearly as possible.

- Although whistle blowers may choose to tell the whistle blowing consultants who they are, the report will never reveal their identity unless the whistle blower specifically allows this, thereby protecting the caller's anonymity; and
- All emails reported to this email address are through a secured mail server and are treated with outmost confidence.

## **REPORTING FRAUD INCIDENTS**

The Accounting Officer will on a regular basis provide feedback to all identified internal stakeholders who could include the Audit and Risk Committee, on its fraud risk management initiatives. Such reports may include the following (depending on which stakeholder reporting to):

Fraud Incidents:

- Summary of number of incidents reported and division impacted:
- Update on investigation status.
- Reporting of fraud incidents including the modus operandi and a trend analysis of which modus operandi is on the increase.
- Commentary on the root causes of the fraud incidents and whether the fraud has been internally or externally perpetrated; and
- Reporting on losses incurred by SWGC.

Ethics:

- Details on any violations to the ethics policies and procedures by staff, service providers, clients or third parties.

Fraud and risk management initiatives:

- Update on the proactive and reactive fraud prevention and detection initiatives implemented.
- Update on SWGC's Fraud Risk Register and any changes to the control environment in mitigating the identified fraud risks.

Training:

Updates on any fraud training and results from surveys/audits on effectiveness of training.

## **11. RESPONSE STRATEGIES**

### **REPORTING FRAUD AND CORRUPTION**

In the responsibility of every employee all incidents of fraud and corruption that may come to his/her attention. Alternatively, such reports can be made by way of submitting a report through the prescribed whistle blowing mechanism of an anonymous call to the toll-free or the email.

The conditions leading to reporting crime may differ from one instance to another, but employees are encouraged to use the internal channels. When offences are reported,

requirements of the PFMA and other related statutes within the sector should be considered to protect the perpetrator's right and dignity and the reputation of the institution.

All reports received will be treated with the requisite confidentiality and will not be disclosed or discussed with parties other than those charged with the investigation into such reports.

### **INVESTIGATING FRAUD AND CORRUPTION ALLEGATION**

All suspected fraudulent activities should be reported via emails written submission to the office of the chairperson of the committee and principal, who will assess the incident and allocate it to an appropriate line manager for preliminary investigation or refer it to internal investigations Unit for a full investigation.

A high-level assessment of the information that is provided will involve the following steps:

- Authentication of the allegation; high-level testing of the allegation.
- Consideration of the source of information; and
- Preliminary consultation with appropriate stakeholders within the organization

SWGCG should consider the following options to respond to the fraud or corruption

- Internal disciplinary enquiry
- Criminal prosecution
- Civil recovery of loss

### **INVESTIGATION**

Investigations will be undertaken by appropriate qualified and experienced persons who are independent of the institution/ section where investigations are required. This may be a senior manager within the institution itself, an internal investigator, external consultant, or a law enforcement agency. All investigations performed and evidence obtained will be in accordance with acceptable practices and legal requirements. Independence and objectivity of investigations are paramount.

### **DISCIPLINARY ENQUIRY**

in instituting an internal disciplinary enquiry against an employee, SWGCG must ensure that disciplinary proceedings take place in accordance with the procedure as set out in the organization's HR policy and manual on disciplinary code.

SWGCG will continually endeavour to remain consistent and efficient in its application of the disciplinary measures. Additional measures will be considered include:

- Regular communication of specific disciplinary standards and misconduct definitions.
- Maintaining a system where the application measures is applied consistently.
- Steps for ongoing training of managers in the application of disciplinary measures.
- Where managers are found to be inconsistent and/or inefficient in the application of discipline, SWGCG will take firm corrective action.
- Publication (within the permissible legal framework) of the outcomes and sanctions of disciplinary actions, including lessons learned. The successful achievement of these initiatives, together with their communication will have a deterrent effect.

During the detailed investigation, simultaneous damage control will be implemented. This could include:

- Suspending the perpetrator to limit further financial losses, destruction of evidence, interference with witnesses, etc.
- Addressing control breakdown to stop the fraud from continuing or to prevent recurrence.

The ultimate outcome of disciplinary proceedings may involve a person/s receiving written warnings or the termination of their services.

### **CRIMINAL PROSECUTION**

Fraud, theft, corruption, forgery matters above the R100 000 threshold, as stated by the PRECCA, should be reported to the South African Police Service (SAPS).

In the event that fraud, theft or corruption was detected, investigated, and warranted disciplinary proceedings, prosecution or action aimed at the recovery of losses will be initiated and the matter will be reported to the SAPS, regardless of the value of the offence.

### **CIVIL RECOVERY**

Where there is evidence of fraud or corruption and there has been a financial loss to the organization, action will be instituted to the recovery any such losses. In respect of civil recoveries, costs involved will be determined to ensure that the cost of recovery is financial beneficial.

## **12. REVIEW OF THE FRAUD RISK MANAGEMENT POLICY.**

SWGC will conduct a review of the Fraud Risk Management Policy to determine the effectiveness thereof. The Audit Committee is ultimately accountable for this review. This policy will be subject to review as and when necessary, but at least once in three (3) years, to ensure its relevance.

Fraud and corruption risk assessment will however be conducted annually, in line with the risk management plan of the College.

## **13. ADOPTION AND COMPLIANCE WITH THE POLICY**

- This policy is effective from the date on which it is adopted by Council.
- All staff of the College are expected to comply with the policy with immediate effect.
- Non-compliance with this policy would lead to a disciplinary sanction.
- Consequences may include:
  - Criminal charges being brought against those who are found to be non-compliant
  - Suspension, and or
  - Dismissal

## **14. AVAILABILITY OF RISK MANAGEMENT POLICY**

A copy of this policy and other relevant documentation should be made available on the College website (QMS).



## **Annexure A - Letter to Suppliers- Declaration 2021F**



Letter to Suppliers-  
Declaration 2021F.pdf