

Fraud policy and response plan

Document type: Policy
Policy Category: Governance

Document number: Rt 378/15

The University has established a 24-hour 'Ethics Hotline' and has for this purpose engaged the services of KPMG. The following communication channels are available should you wish to make use of this service (with the option of remaining anonymous should you so prefer):

- A toll-free telephone number: 0800 200 651
- A toll-free fax number: 0800 200 796
- A secure email address: fraud@kpmg.co.za
- A free-post address: BNT 371, PO Box 14671, Sinoville, 0129
- A web-based address: <https://rea.msvcs.kpmg.com/ggt-anonym/Entry/QuestionnaireEntry.aspx?AnswerSetId=2725512&SessionId=098ecb1c3516458889a628ab676b933a>

CONTENTS

1. GLOSSARY	3
2. BACKGROUND	8
3. SCOPE OF THE POLICY	9
4. THE POLICY	9
5. REPORTING PROCEDURES AND RESOLUTION OF REPORTED INCIDENTS	9
6. CONFIDENTIALITY	12
7. PUBLICATION OF SANCTIONS	12
8. PROTECTION OF WHISTLE-BLOWERS	12
9. APPLICATION OF PREVENTION CONTROLS AND DETECTION MECHANISMS	13
10. CREATING AWARENESS	13
11. ADMINISTRATION	13

1. GLOSSARY

Throughout this document, unless otherwise stated, the words in the first column below have the meanings stated opposite them in the second column or below them, as the case may be (and cognate expressions shall bear corresponding meanings):

- 1.1 Act : The Protected Disclosures Act 26 of 2000;
- 1.2 Policy : Fraud Policy and Response Plan of the University of Pretoria;
- 1.3 SAPS : The South African Police Service; and
- 1.4 UP : The University of Pretoria;
- 1.5 Fraud and corruption includes, but is not limited to, the following legal definitions –
 - 1.5.1 Fraud, i.e. the unlawful and intentional making of a misrepresentation which causes actual prejudice or which is potentially prejudicial to another.
 - 1.5.2 Theft, i.e. the unlawful and intentional appropriation of movable corporeal property, including information in electronic format which belongs to and is in the possession of another; which belongs to another but is the perpetrator's own possession; or which belongs to the perpetrator but is in the possession of another person who has a right to possess it and where such right legally prevails against the perpetrator's own right of possession.
 - 1.5.3 Offences in respect of *corrupt activities* as defined in the Prevention and Combating of Corrupt Activities Act 12 of 2004, including but not limited to:
 - 1.5.3.1 The general offence of corruption (section 3), which can be summarised as directly or indirectly accepting or agreeing or offering to accept any gratification from any other person, whether for the benefit of himself/herself or for the benefit of another person; or giving or agreeing or offering to give to any other person any gratification, whether for the benefit of that other person or for the benefit of another person, in order to act, personally or by influencing another person to act, in a manner –

- (a) that amounts to the illegal, dishonest, unauthorised, incomplete, or biased; or misuse or selling of information or material acquired in the course of the exercise, carrying out or performance of any powers, duties or functions arising out of a constitutional, statutory, contractual or any other legal obligation;
- (b) that amounts to the abuse of a position of authority; breach of trust; or violation of a legal duty or set of rules;
- (c) designed to achieve an unjustified result; or
- (d) that amounts to any other unauthorised or improper inducement to do or not to do anything.

1.5.3.2 Specific corrupt activities (sections 4-16), relating to –

- (a) public officers;
- (b) foreign public officials;
- (c) agents;
- (d) members of the legislative authority;
- (e) judicial officers;
- (f) members of the prosecuting authority;
- (g) receiving or offering of unauthorised gratification from or to a party to an employment relationship;
- (h) witnesses and evidential material during certain proceedings;
- (i) contracts;
- (j) procuring and withdrawal of tenders;
- (k) auctions;
- (l) sporting events; or
- (m) gambling games or games of chance.

1.5.3.3 Miscellaneous offences relating to a possible conflict of interest and other unacceptable conduct (sections 17-19), namely:

- (a) acquisition or holding of a private interest by any public officer in any contract, agreement, transaction or investment emanating from or connected with the public body in which he/she is employed;
- (b) unacceptable conduct relating to witnesses; or

- (c) intentional interference with, hindering or obstruction of the investigation of an offence.

1.5.3.4 Other offences relating to corrupt activities (sections 20-21), namely:

- (a) being an accessory to or after an offence;
- (b) attempt, conspiracy and inducing another person to commit an offence; or
- (c) failure to report corrupt transactions (section 34).

1.5.4 Contraventions of the Higher Education Act 101 of 1997 (as amended).

1.5.5 Cyber-crime as defined in the Electronic Communications and Transactions Act 25 of 2002, including but not limited to:

1.5.5.1 Unauthorised access to, interception of or interference with data in terms of section 86(1) can be summarised as the following:

- (a) the intentional accessing or intercepting of any data without authority or permission to do so;
- (b) the intentional and unauthorised interference with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective;
- (c) to unlawfully produce, sell, offer to sell, procure for use, design, adapt for use, distribute or possess any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or to perform any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section of the said act;
- (d) to utilise any device or computer program mentioned above in order to unlawfully overcome security measures designed to protect such data or access thereto; or
- (e) to commit any act described above with the intent to interfere with access to an information system so as to constitute a denial, including partial denial, of service to legitimate users.

1.5.5.2 Computer-related extortion, fraud and forgery in terms of section 87(1) can be summarised as meaning to perform an act or to threaten to perform an act as described in section 86 for the purpose of obtaining any unlawful proprietary advantage by undertaking to cease or desist from such action, or by undertaking to restore any damage caused as a result of those actions. This further includes any of the acts described in section 86 performed for the purpose of obtaining any unlawful advantage by causing fake data to be produced with the intent that it be considered or acted upon as if it were authentic.

1.5.5.3 Attempt, aiding and abetting can be summarised as an attempt to commit any of the offences referred to in sections 86 and 87. This further includes any act performed by a person in order to aid and abet someone to commit any of the offences referred to in sections 86 and 87.

1.5.6 Irregularities related to –

1.5.6.1 Systems issues: i.e. where an existing process/system is prone to abuse by employees, students, the public or other stakeholders, e.g. –

- (a) forging UP degrees;
- (b) abuse of leave;
- (c) abuse of the system of “flexi-time”;
- (d) abuse of the system of “limited private practice” and “external work”;
- (e) non-compliance with delegated authority limits;
- (f) manipulation of pass rates by fraudulently altering student marks;
- (g) procurement fraud;
- (h) abuse of the system of general claims or claims for services rendered;
- (i) deliberate material non-compliance with policies and procedures;
- (j) falsification of qualifications;

- (k) abuse or mismanagement of development funds from donors / external funders;
- (l) mismanagement of long-term investments;
- (m) mismanagement of monies in suspense or dormant accounts;
- (n) fraudulent raising of funds by students/employees;
- (o) disclosing confidential information, e.g. examination papers, research etc. to external parties;
- (p) theft of blank cheques;
- (q) any other fraudulent systems issues not specifically mentioned above; or
- (r) irregular use of consultants.

1.5.6.2 Financial issues: i.e. where individuals or entities have fraudulently obtained money from UP, e.g. through –

- (a) theft of money;
- (b) fraudulent travel and general claims;
- (c) submission of claims for services rendered for activities which are part of the staff member's existing employment relationship with UP;
- (d) contractors invoicing for work not done;
- (e) contractors "fronting" (acting as a front for another person or entity);
- (f) fraudulent reallocation of funds;
- (g) opening and/or operating a bank account in the name of UP without the prior written authorisation of Council;
- (h) self-approval of expenditure, whether through the general claims or procurement process, without appropriate line manager authority;
- (i) simulating employment ("ghost employees"); or
- (j) any other fraudulent financial issues not specifically mentioned above.

1.5.6.3 Equipment and resource issues: i.e. where equipment of UP is utilised for personal benefit or stolen, e.g. by –

- (a) theft of assets, e.g. art, laboratory equipment, computer equipment etc;

- (b) deliberate damaging, substandard workmanship, unnecessary repairs/orders or destruction of property by facilities and services contractors in order to secure additional work;
- (c) use of UP resources and equipment for private gain; or
- (d) any other fraudulent equipment and resource issues not specifically mentioned above.

1.5.6.4 Other issues: i.e. activities undertaken by UP employees and students which contravene existing policies and/or established ethical standards, e.g. –

- (a) copyright infringements;
- (b) committing plagiarism;
- (c) collusion between students and lecturers;
- (d) writing of exams by one student on behalf of another;
- (e) creating or failing to disclose a conflict of interest;
- (f) non-disclosure of private work;
- (g) installation of pirated or illegal software or other electronic content (e.g. DVDs, music, etc.);
- (h) misconduct that constitutes research fraud such as fabrication or inappropriate manipulation of research data, multiple publication of the same content with different titles, ghost-writing, misappropriation of research data or any other research misconduct; or
- (i) any other fraudulent issues not specifically mentioned above.

2. BACKGROUND

2.1 The aim of the Policy is to formalise UP's position with regard to fraud and corruption and to reinforce existing systems, policies and procedures aimed at deterring, preventing, detecting, reacting to and reducing the impact of fraud and corruption at the University.

2.2 Furthermore, the purpose of this document is to confirm that UP supports and fosters a culture of zero tolerance to fraud and corruption in all its activities.

- 2.3 This policy should be read with the University's Whistle-blowers Policy, as well as the Internal Audit Policy and Internal Audit Charter, as the Internal Audit function plays a role in the identification and investigation of reports of fraud and whistle-blowing.

3. SCOPE OF THE POLICY

- 3.1 The Policy is applicable to all allegations, attempts and incidents of fraud and corruption which impact or may potentially have an impact on UP.
- 3.2 All employees and the management of UP, or any entity controlled by UP (including students), must comply with the spirit and content of this Policy.

4. POLICY STATEMENT

- 4.1 The basis of this policy is zero tolerance to fraud and corruption. In addition, all alleged cases of fraud and corruption shall be investigated and followed up by the application of all remedies available within the full extent of the law and the implementation of appropriate prevention and detection measures (controls). These controls include the existing financial and other controls and checking mechanisms as prescribed in the systems, policies and procedures of UP.
- 4.2 The efficient application of instructions contained in the regulations, policies and procedures of UP is one of the most important duties of every employee in the execution of his/her daily tasks.

5. REPORTING PROCEDURES AND RESOLUTION OF REPORTED INCIDENTS

- 5.1 What should an employee do if he/she suspects fraud and corruption?
- 5.1.1 It is the responsibility of every employee to immediately report any alleged incident of fraud and corruption to his/her immediate manager, or to the Registrar. Should it be suspected that a member of Senior Management may be involved, the report should be submitted to the Vice-Chancellor and Principal or the Chairperson of the Audit, IT and Risk Management Committee.
- 5.1.2 Managers are responsible for the detection, prevention and investigation of fraud and corruption and shall report every incident and allegation of fraud and

corruption to the relevant individual mentioned in paragraph 5.1.1 above, who shall initiate an investigation into the matter.

5.1.3 Should an employee wish to report an alleged incident of fraud and corruption (anonymously or otherwise), he/she may also avail himself/herself of the various communication channels or avenues available to employees, as indicated on the cover page of this policy document. The “Ethics Hotline” facility is available on a 24-hour basis.

5.2 What should a student, member of the public or a provider of goods and/or services do if he/she suspects fraud and corruption?

5.2.1 UP encourages every student, member of the public or provider of goods and/or services who suspects fraud and corruption in the UP environment to report such suspicion to the Registrar or the Vice-Chancellor and Principal who will deal with the matter in accordance with the relevant procedure as set out in paragraph 5.1 above.

5.2.2 Students, members of public or providers of goods and/or services can also report such allegations (anonymously or otherwise) by following one of the various communication channels or avenues available to all complainants as indicated on the cover page of this policy document.

5.3 How will allegations of fraud and corruption be dealt with?

5.3.1 With regard to issues raised by an employee, student, member of the public or provider of goods and/or services, the action taken will depend on the nature of the concern and the procedures outlined in the University’s Whistle-blowers Policy. The matters raised shall be screened and evaluated and may subsequently:

5.3.1.1 be investigated internally; and/or

5.3.1.2 referred to another law enforcement agency.

5.3.2 Any fraud and corruption committed by an employee or any other person shall be pursued by thorough investigation and to the full extent of the law, including (where appropriate) consideration of –

- 5.3.2.1 in the case of employees, taking disciplinary action within a reasonable period of time after the incident;
 - 5.3.2.2 instituting civil action to recover any loss;
 - 5.3.2.3 initiating criminal prosecution by reporting the matter to the SAPS or any other relevant law enforcement agency; and/or
 - 5.3.2.4 any other appropriate legal remedy available.
- 5.4 Managers shall ensure that compensation for any loss or damage suffered by UP as a result of any reported act or omission, which can be classified as fraudulent and corrupt, by an employee, student or any other person, who falls under the authority of such manager, is recovered from such employee, student or other person should he/she be found to be liable for such loss or damage.
- 5.5 UP, upon receiving a report of fraud and corruption from a whistle-blower, will:
 - 5.5.1 enter the complaint in the Whistle-blowing Register;
 - 5.5.2 initiate a preliminary enquiry/review on the allegations; and
 - 5.5.3 should the results of the preliminary review indicate the need for further investigation, refer the matter to the appropriate Department, internal or external auditors, or any other relevant party.
- 5.6 UP accepts that every person, including an employee or student or supplier or external party, who reported the alleged fraud and corruption needs to be assured that the matter has been properly addressed. Thus, subject to legal constraints, information about the outcome of any investigation may be disseminated on a "need to know" basis.
- 5.7 UP shall ensure that a fraud and corruption information system is developed for the following purposes:
 - 5.7.1 recording of all allegations;
 - 5.7.2 tracking the progress made in the management of allegations;

5.7.3 facilitating the early identification of systemic weaknesses and recurring risks and informing managers and employees of systemic weaknesses and recurring risks; and

5.7.4 where appropriate and not subject to privilege, providing feedback to employees and/or whistle-blowers on the management of allegations.

6. CONFIDENTIALITY

6.1 All information relating to fraud and corruption which has been received and investigated shall be treated confidentially. The progress made with investigations shall be handled in a confidential manner and shall not be disclosed or discussed with any persons who have no legitimate claim to such information. This is important in order to avoid damaging the reputation of a suspected person who may subsequently be found to be innocent of the alleged wrongful conduct.

6.2 No person shall supply any information with regard to allegations or incidents of fraud and corruption to the media without the express permission of the Vice-Chancellor and Principal or the Chairperson of the Audit, IT and Risk Management Committee.

7. PUBLICATION OF SANCTIONS

The Vice-Chancellor and Principal or the Chairperson of the Audit, IT and Risk Management Committee shall decide whether any information relating to corrective actions taken or sanctions imposed in respect of incidents of fraud and corruption should be brought to the direct attention of any person or made public by any other means.

8. PROTECTION OF WHISTLE-BLOWERS

8.1 An employee, student or external party who reports suspected fraud and corruption may remain anonymous should he/she so desire.

8.2 In line with the Whistle-blowers Policy and relevant legislation, no person shall suffer any penalty or retribution for the reporting in good faith of any suspected or actual incident of fraud and corruption which purportedly or in fact occurred within UP.

8.3 Managers should discourage employees or other persons from making allegations which are false and made with malicious intent. In instances where such allegations are proven to be untrue and malicious or vexatious, the person who made the allegations shall be subjected to firm disciplinary action, while appropriate action shall be taken in the case of external parties.

9. APPLICATION OF PREVENTION CONTROLS AND DETECTION MECHANISMS

In respect of all reported incidents of fraud and corruption, management shall immediately review and, where possible, improve the effectiveness of the controls that have been breached in order to prevent similar irregularities from taking place in future.

10. CREATING AWARENESS

Managers shall be responsible for ensuring that all employees under their control are made aware of and receive the relevant policy documentation.

11. ADMINISTRATION

The custodian of the Policy is the Head: Unit for Internal Audit who shall be responsible for the administration, revision and interpretation of the Policy.

The Policy shall be reviewed every three years and appropriate changes effected, should these be required.

12. DOCUMENT METADATA

Document number:	<i>Rt 378/15</i>
Document version:	<i>Rt 378/15 newly approved version Replacing Rt 669/11</i>
Document approval authority:	<i>Executive</i>
Document approval date:	<i>3 November 2015</i>
Document owner:	<i>Unit for Internal Audit</i>
Document author(s):	<i>Head: Unit for Internal Audit</i>
Date:	<i>3 December 2015</i>
Visibility:	
Display on staff intranet	√
Display on student intranet	√
Display on public web	√