

## Fraud Response Policy

**Category:** Finance  
**Last Modified:** March 2009  
**Review Date:** June 2013  
**Approved By:** Director of Finance  
**Contact Person:** Financial Reporting and Budgeting Manager, Extn 45559

### **Introduction:**

The University defines fraud as:

“Any action deliberately designed to cause loss to the University, or to obtain any unauthorised benefit, whether or not this is received personally, or by others.”

More specifically, this includes, but is not limited to:

- Forgery or alteration of cheques, drafts, securities, or similar documents.
- Any misappropriation of funds, securities, supplies or any other asset.
- Any irregularity in the handling or reporting of financial transactions.
- Misappropriation of furniture, fixtures or equipment.
- Seeking or accepting anything of material value (more than \$100) from vendors, consultants or contractors doing business with the University without the authorisation of the Chief Financial Officer.
- Unauthorised use or misuse of property, equipment, materials or records (including academic records)
- Disclosing confidential or proprietary information, including intellectual property, to outside partners.
- Any computer-related activity involving the alteration, destruction, forgery or manipulation of data for fraudulent purposes, or misappropriation of software.
- Any claim for reimbursement or expenses that are not made for the exclusive benefit of the University.
- Dishonest use of a University Purchasing card.
- The failure to disclose any conflict of interest in processes for the goods and services to the University.
- Private use of University resources outside the normal usage (refer to the IT website for IT details).

The University has a zero tolerance to fraud. As well as seeking to reduce both the opportunity and scope for fraud, the University is also committed to taking prompt action to fully investigate and address any suspected cases, whether carried out by staff, students, suppliers or other partners. Sections 2 to 9 of this document define the authority levels, responsibilities for action, and reporting lines in the event of a suspected fraud or irregularity.

## **Contents:**

1. [Initiating Action](#)
2. [Prevention of Further Loss](#)
3. [Recovery of Losses](#)
4. [Reporting to Senior Management](#)
5. [Reporting to the Council Audit and Risk Committee](#)
6. [References for staff Disciplined and Prosecuted for Fraud](#)
7. [Whistle-Blower Protection](#)
8. [Media Issues](#)
9. [Review of the Fraud Response Policy](#)

## **Policy Statement:**

The use of the policy should enable the University to:

- Prevent further loss
- Establish if there is a case for criminal or disciplinary action
- Retain any relevant evidence
- Minimise and recover losses
- Review the reasons for the incident, the measures taken to prevent a recurrence, and any action needed to strengthen future responses to fraud
- Keep all personnel with a need to know suitably informed about the incident and the institution's response
- Assign responsibility for investigating the incident
- Establish circumstances in which external specialists should be involved; and
- Where appropriate, notify the police and establish lines of communication with them
- Deal with requests for references for employees disciplined or prosecuted for fraud.

## **Policy and Procedures:**

### **1. Initiating Action**

Suspicion of fraud or irregularity may be captured through a number of means, including the following:

- requirement of this policy for all members of staff to report fraud or irregularity to their immediate supervisor, or one level above this if necessary
- public interest disclosure procedure
- planned audit work; and

- operation of proper procedures.

All actual or suspected incidents should be reported without delay to the Chief Financial Officer, who should, within 24 hours, hold a meeting of a Fraud Response Group (FRG) to decide on the initial response. This group consists of:

- Chief Financial Officer
- Human Resources Director; and
- The University Registrar

If the actual or suspected incident concerns or implicates the Financial Reporting and Budget Manager, it should be reported without delay to the Chief Financial Officer who will initiate the procedures for investigation set out in this Policy.

The FRG will decide on the action to be taken. This will normally be a review led by the Financial Reporting and Budget Manager. It may be necessary to involve the University Senior Security Officer at the time action is to be initiated. If the size or seriousness of the incident(s) warrants, a special review will be led by the University internal auditors who will make recommendations to the FRG about further action. This would include any recommendation(s) about police action. It may involve a change in internal audit resources from planned audits. Some special investigations may require the use of technical expertise, which the internal auditors may not possess. In these circumstances, external specialists may be appointed to lead, or contribute to, the investigation. If the FRG decides that a special investigation is not required, the outcome shall be reported to the complainant and other persons appropriate at the time.

Where an investigation is to take place, and the matter implicates any of the persons referred to in paragraph 2 above, another person with senior management responsibility shall be appointed by the Group.

The FRG will also decide what information should be conveyed to the University Audit and Risk Committee, the Police, and the University Insurance brokers.

All information received will be treated confidentially. It must be appreciated, however, that the investigation process may reveal the source of the information, or a statement by the individual may be required as part of the evidence. Investigation results will not be disclosed or discussed with anyone other than those who have a legitimate need to know. This is important in order to avoid damaging the reputations of persons suspected but subsequently found innocent of wrongful conduct, and to protect the University from potential civil liability.

Members of the FRG will have:

- free and unrestricted access to all University records and premises, whether owned or rented; AND
- the authority to examine, copy, and/or remove all, or any portion of the contents of files, desks, cabinets, and other storage facilities on the premises without prior knowledge or consent of any individual who may use or have custody or any such items or facilities, when it is within the scope of their investigation.

A major fraud event would require the development of a Fraud Response Plan (FRP) specific to that event (refer to Appendix 2).

## **2. Prevention of Further Loss**

- 2.1 Where initial investigation provides reasonable grounds for suspecting a member or members of staff of fraud, the FRG will decide how to prevent further loss. This may require the suspension, with or without pay, of the suspects. It may be necessary to plan the timing of suspension to prevent the suspects from destroying or removing evidence that may be needed to support disciplinary or criminal action.
- 2.2 In these circumstances, the suspect(s) should be approached unannounced. They should be supervised at all times before leaving the University's premises. They should be allowed to collect personal property under supervision, but should not be able to remove any property belonging to the University. Any security passes and keys to premises, offices and furniture should be returned.
- 2.3 The University Senior Security Officer should advise on the best means of preventing future access to the University, including while suspects are suspended. If appropriate, the issues should be escalated to the Director of Facilities Management. Similarly, the ICTS Director should be instructed to withdraw access permissions to the University's computer systems.
- 2.4 The Chief Financial Officer should consider whether or not it is necessary to investigate systems other than that which has given rise to suspicion, through which the suspect may have had opportunities to misappropriate the University's assets.

## **3. Recovery of Losses**

- 3.1 The University will follow disciplinary procedure against any member of staff who has committed fraud, and will also normally pursue the prosecution of any such individual.
- 3.2 Recovering losses is a major objective of any fraud investigation, and the amount of any loss will be quantified insofar as this is possible. Repayment of losses should be sought in all cases.
- 3.3 Where the loss is substantial, legal advice will be obtained about the need to freeze the suspect's assets through the court, pending conclusion of the investigation. Legal advice should also be obtained about prospects for recovering losses through the court, where the perpetrator refuses payment. The University would normally expect to recover costs in addition to losses.

## **4. Reporting to Senior Management**

Where a suspected fraud is being investigated, the Financial Reporting and Budget Manager will provide a confidential report to the Chief Financial Officer at least monthly, unless the report recipient requests a lesser frequency. The scope of the report shall include:

- i. Quantification of losses
- ii. Progress with recovery action
- iii. Progress with disciplinary action
- iv. Progress with criminal action
- v. Estimate of resources required to conclude the investigation; and
- vi. Actions taken to prevent and detect similar incidents.

## **5. Reporting to the Council Audit and Risk Committee**

On completion of the investigation, a written report shall be submitted to the Audit and Risk Committee containing:

- i. A description of the incident, including the value of any loss, the people involved, and the means of perpetrating the fraud
- ii. The measures taken to prevent a recurrence
- iii. Any action needed to strengthen future responses to fraud.

## **6. References for Staff Disciplined or Prosecuted for Fraud**

Full details of the investigation will be attached to the personnel files of the staff involved.

Any request for a reference for a member of staff who has been disciplined, or prosecuted for fraud, shall be referred to the Director of Human Resources who shall prepare any reply having regard to employment and other relevant law. It is a requirement that a specific reference will be made to the fraud episode(s).

## **7. Whistle-Blower Protection**

No employer or person acting on behalf of an employer shall:

- dismiss or threaten to dismiss an employee
- discipline or suspend or threaten to discipline or suspend an employee
- intimidate or coerce an employee, because the employee has acted in accordance with the requirements of the policy. The violation of this section will result in discipline up to and including dismissal.

## **8. Media Issues**

Any staff person or elected member contacted by the media with respect to an audit investigation shall refer the media to the Corporate Affairs Manager. The alleged fraud or audit investigation shall not be discussed with the media by any person other than through the Corporate Affairs Manager.

If the University's internal or external auditors are contacted by the media regarding an alleged fraud or audit investigation, then he/she will consult with the Chief Financial Officer and the Corporate Affairs Manager before responding to a media request for information or interview.

The Director of Communications will draft media messages and recommend an appropriate spokesperson if required, for the FRG to consider.

## **9. Review of the Fraud Response Plan**

This plan will be reviewed at least bi-annually, or after any major event, by the Financial Reporting and Budget Manager to ensure that all appropriate procedures are in place. Any need for change will be referred to the Fraud Response Group for consideration, to the Chief Financial Officer for consideration, and then to the Audit and Risk Committee for their information.

## **Related Policies, Procedures and Forms:**

- [Crimes Act 1961](#)
- [Protected Disclosures Act 2000](#)
- [Protected Disclosures Act: Internal Procedures and Code of Conduct](#)

## **Appendices:**

- Appendix 1: Guidance for the Prevention of Fraud in Areas of Risk
- Appendix 2: Key Components of a Fraud Response Policy (FRP) in relation to a specific major fraud event

<b>Version Control Table</b>		
<b>Action</b>	<b>Approval Body</b>	<b>Date Amended</b>
Full Review	Chief Financial Officer	4 March 2009

© *This policy is the property of the University of Canterbury.*

# APPENDIX 1

## Guidance for the Prevention of Fraud in Areas of Risk

### 1. Cash

Cash can involve cash boxes, cash registers, takings at bars, residences, catering outlets and vending machines. Management of cash should include the following:

- Segregation of duties. Systems should prevent one person from receiving and recording and also banking cash. The system should incorporate additional supervisory management, and spot checks. Segregation of duties should continue during periods of leave or sickness absence.
- Reconciliation procedures. An independent record of cash received and banked must be kept, and staff documents used in reconciliation processes.
- Receipts must be issued for all cash received, to provide an audit trail.
- Physical security measures are also necessary, including key pad controlled cashiers' offices and safes. The University usually suffers losses because cash is left unsecured, often despite ready availability of safes. Keys and access codes should also be kept secure.
- Frequent banking, preferably daily.
- Use alternatives to cash, including purchasing cards, cheques, direct debits, and direct credits.

### 2. Cheques

It is possible for cheques to be completed in ways which facilitate opportunist fraud. Sometimes such cheques can be intercepted by people who falsify payee and value details using sophisticated techniques. Debtors may also be told to make cheques payable to a private account, possibly using an account name which is similar to the University's. Preventative measures include:

- Physical security. Unused, completed and cancelled cheques must be held in secure facilities. If cheques are destroyed, more than one staff member should be present, and a record of the serial numbers should be maintained.
- Frequent bank reconciliations. Accounts must be reconciled promptly, preferably daily.
- Segregation of duties. Receipting and reconciliation activities must be kept separate.
- Clear instructions to debtors about correct payee details and the address to which cheques should be sent. The address should normally be the Financial Services Unit, not the department which has provided the goods or services.
- Central opening of all mail delivered to Financial Services Unit.
- Rotation of staff responsibilities.
- Training in secure completion of cheques.
- Use of electronic funds transfer (EFT) as an alternative to cheques.
- Six monthly checks with local banks for accounts which include the University's name.

### **3. Purchasing ledger**

Preventative measures include:

- Minimising little used or unusual account codes.
- Ensuring that all account codes are effectively monitored by line management.
- Segregation of duties.
- Secure management of the creditors' master file, including segregating the originating and approval of new or amended data.
- Requiring purchase orders for the procurement of all goods and services except where services are not usually ordered (e.g. electricity), variable (e.g. travel supply) or the use of a purchasing card is not appropriate (e.g. design consultancy work).
- Suppliers should be vetted to establish that they are genuine and reputable companies before being added to lists of authorised suppliers.

## APPENDIX 2

### Key Components of a Fraud Response Plan (FRP) in Relation to a Specific Major Fraud Event

1. The plan should be in writing and as part of its development involve an appropriate level of professional consultation. The Chief Financial Officer will approve the plan.
2. The plan should consider any internal arrangements felt necessary to assist in any external criminal investigation conducted by the Police.
3. The plan should set out who will control an internal fraud investigation in the event that investigation referrals to the Police are declined. If this occurs it will be necessary to develop and have approved a separate internally controlled fraud investigation process.
4. The plan should set out who will be involved and what their role will be throughout the fraud response process. Communication with parties outside of this process should be on a strict need to know basis.
5. A communication strategy should be developed by the Corporate Affairs Manager as part of the plan. This strategy should cover:
  - Who will make external statements to the media and liaise with parties specifically involved during the course of any Police or internal fraud investigation;
  - The handling of internal communications where an employee is suspected to be implicated and the Police have agreed to carry out a criminal investigation;
  - Liaison arrangements for Police or external investigators or legal advisors; and
  - The nature and type of internal advice or communications once any investigation process has been completed or the event concluded.
6. The plan should consider options for the counselling of affected employees and handling of local morale issues that could arise during and after any Police or internal fraud investigation.
7. The plan should require a post-event analysis of outcomes. This process should involve identification of the lessons to be learnt, consideration of improvements to existing internal controls and procedures and final report back to the Chief Financial Officer.