UC Policy Library

Fraud Response Policy and Procedures

Last Modified	August 2019
Review Date	August 2020
Approval Authority	Chief Financial Officer
Contact Officer	Senior Accountant Project Assurance – Financial Services

Introduction

This policy sets out the University's position and methods of managing and addressing instances where an alleged fraud may have taken place.

Contents

Definitions

Fraud – 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 Executive Director/Chief Financial Officer (CFO).
- 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 is 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 goods and services to the University.
- Private use of University resources outside the normal usage (refer to *IT Services (University Information and Technology Services website)* for IT details).

Member/s of the Public – those that are neither staff nor students.

Staff or staff member – for the purposes of this policy, the definition of "staff" or "staff member" extends to cover all persons working at, for, or on behalf of, the University (whether paid or unpaid), including but not limited to, contractors, subcontractors and their employees, adjunct appointees, Erskine visitors, consultants, guest lecturers, interns and volunteers.

Student – a person who is currently enrolled as a student at the University, either directly or through official arrangements with another organisation.

University Document – Any document bearing the University crest and/or the signature of a University staff member; any document purporting to represent the views of the University or document trying to obtain benefits from the University e.g., an email, form seeking to obtain a benefit from the University.

Policy Statement

The University has zero tolerance to fraud.

The University will implement controls for the prevention and detection of fraud. The University will also take steps to ensure that staff (including those providing services to the University), students and alumni, know of their obligations in relation to fraud, including identification and reporting of suspected fraud.

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

The use the following procedures 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;
- Where appropriate, notify the police and establish lines of communication with them;
- Deal with requests for references for employees disciplined or prosecuted for fraud.

Procedures

1. Initiating Action

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

- The 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;
- The public interest disclosure procedure;
- Planned audit work;
- The operation of proper procedures.

All actual or suspected incidents not involving University documents or , should be reported without delay to the Executive Director/Chief Financial Officer (CFO), who should, within 24 hours, hold a meeting of a Fraud Response Group (FRG) to decide on the initial response. This group consists of the

- CFO,
- Executive Director, Human Resources, and
- University Registrar.

If the actual or suspected incident concerns or implicates the Financial Controller, it should be reported without delay to the CFO who will initiate the procedures for investigation set out in this document.

If the actual or alleged fraud does involve University documents, the reporting and investigation procedures will be based on the alleged offender:

- **Student** – All actual or alleged cases of documentary fraud committed by an enrolled student should be reported to the University Proctor in the first instance. Documentary fraud constitutes a 'breach of discipline' as per the *Discipline Regulations (University Regulations website)* and as such the Proctor is responsible in the first instance for investigation of the matter. The University Registrar should also be notified in the first instance, as the relevant member of the Fraud Response Group (FRG).

  In instances where the investigation reveals the possibility of an offence under sections 15-20 of the *Summary Offences Act 1981 (New Zealand Legislation website)* or sections 255-265 of the *Crimes Act 1961 (New Zealand Legislation website)*, the Proctor may report the matter to the Police.

  In accordance with section 4(c) of the *Discipline Regulations (University Regulations website)*, proven or admitted breaches of discipline will be noted on the University Discipline Register for a period of no more than seven years unless within that time there is a further occurrence.

- **Staff member** – All actual or alleged cases of documentary fraud committed by a staff member should be reported to the relevant Senior Management Team (SMT) Member in the first instance. The SMT Member is responsible in the first instance for investigation of the matter. The Executive Director, Human Resources should also be notified, as the relevant member of the Fraud Response Group (FRG).

- **Alumni** – All actual or alleged cases of documentary fraud committed by an alumnus/alumna of the University should be reported to the Registrar in the first instance. Following preliminary investigation, the Registrar may refer the matter to the Police for appropriate processing.

  Where an alumnus/alumna is convicted following prosecution the University will record this on their permanent student file held internally for a period of seven years unless within that time there is a further occurrence.

  Members of the Public – As with alumni, all actual or alleged cases of documentary fraud committed by a member of the general public should be reported to the Registrar in the first instance. Following preliminary investigation, the Registrar may refer the matter to the Police for appropriate processing.

a) Role of the FRG

The FRG will decide on the action to be taken in most instances. This will normally be a review led by the Financial Controller. It may be necessary to involve the Manager, Security and Campus Community Support at the time action is to be initiated.

Where the fraud involves University documents, the University Registrar will advise FRG. When the fraud involves a student the FRG will not usually need to take further action.

However, it should retain a watching brief of the identification of, and appropriate action taken in response to allegations of fraudulent behaviour.

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 appropriate persons at the time.

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

The FRG will also decide what information should be conveyed to the University Audit and Risk Committee, the Police and the University's insurance brokers/insurers.

b) Confidentiality of Information

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;
- Will have 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 of any such items or facilities, when it is within the scope of their investigation; and
- Are required to keep discussions and information confidential.

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

2. Prevention of Further Loss

- 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 suspect/s. It may be necessary to plan the timing of suspension to prevent the suspect/s from destroying or removing evidence that may be needed to support disciplinary or criminal action.

- 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.
- The Manager, Security and Campus Community Support 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 Executive Director of Learning Resources. Similarly, the Chief Information Officer (CIO) should be instructed to withdraw access permissions to the University's computer systems.

  The CFO should consider whether or not it is necessary to investigate systems other than that which has given rise to suspicion, through which the suspect/s may have had opportunities to misappropriate the University's assets.

3. Recovery of Losses

- The University will follow disciplinary procedures against any member of staff who has committed fraud, and will also normally pursue the prosecution of any such individual.
- 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.
- 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 the prospects for recovering losses through the court, where the perpetrator refuses repayment. 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 Controller will provide a confidential report to the CFO at least monthly, unless the report recipient requests a lesser frequency. The scope of the report shall include,

- quantification of losses,
- progress with recovery action,
- progress with disciplinary action,
- progress with criminal action,
- estimate of resources required to conclude the investigation, and
- 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

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

6. References for Staff Disciplined or Prosecuted for Fraud

Full details of the investigation/s will be attached to the personnel file/s 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 Executive Director, 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; and/or
- Intimidate or coerce an employee because the employee has acted in accordance with the requirements of this policy. The violation of this section will result in discipline up to and including dismissal.

8. Media Issues

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

If the University's internal or external auditors are contacted by the media regarding an alleged fraud or audit investigation, then they will consult with the CFO and the Communications and External Relations Manager before responding to a media request for information or interview.

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

Related Documents and Information

Legislation

- Contract and Commercial Law Act 2017 (New Zealand Legislation website)
- Crimes Act 1961 (New Zealand Legislation website)
- Protected Disclosures Act 2000 (New Zealand Legislation website)
- Summary Offences Act 1981 (New Zealand Legislation website)

UC Regulation

- Discipline Regulations (University Regulations website)

UC Policy Library

- Protected Disclosures Act – Internal Procedures and Code of Conduct (PDF,416KB)
- Staff Code of Conduct (PDF,429KB)
- Student Code of Conduct (PDF,220KB)

UC Website and Intranet

- IT Services (University Information and Technology Services website)

Appendices

- Appendix 1: Guidance for the Prevention of Fraud in Areas of Risk
- Appendix 2: Key Components of a Fraud Response Plan in Relation to a Specific Major Fraud Event

Document History and Version Control Table			
Version	**Action**	**Approval Authority**	**Action Date**
For document history and versioning prior to 2013 contact ucpolicy@canterbury.ac.nz			
1.00	Major review of document and conversion into new template. Updated hyperlinks.	Chief Financial Officer	Sep 2013
1.01	Hyperlinks and titles updated.	Policy Unit	Jul 2014
2.00	Scheduled review by Financial Controller.	Policy Unit	Aug 2015
2.01	Inserted new hyperlink.	Policy Unit	Oct 2015
2.02	'Communications and Stakeholder Manager' updated to 'Communications and Engagement Manager'.	Policy Unit	Feb 2016
3.00	Scheduled review by Contact Officer.	Policy Unit	May 2016
3.01	Unscheduled review, inclusion of electronic signature guidelines to Appendix 1.	Policy Unit	April 2017

3.02	Unscheduled review by PU, incorporating the Documentary Fraud Response Policy procedures	Chief Financial Officer	June 2017
3.03	Change to staff definition	Policy Unit	July 2017
4.00	Scheduled review by CO, changes to appendices to reflect legislation change	Change of title to include procedures	Aug 2019

This document remains in force until it is updated

UNIVERSITY OF CANTERBURY
Te Whare Wānanga o Waitaha
CHRISTCHURCH NEW ZEALAND

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.
- The use of 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 opportunistic 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 the Financial Services Unit.

- Rotation of staff responsibilities.
- Training in secure completion of cheques.
- The 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.

4. Electronic Signatures

For Staff

- The signature must adequately identify the signatory and approval of information to which the signature relates under *s 226* of the *Contract and Commercial Law Act 2017*. Therefore, the individual staff member wishing to sign with an electronic signature should create the signature and limit its use to official University documents or purposes, and legal documents or legal requirements where a signature is required.

  For example, “official” University use may be on official University correspondence to staff, students or on official University websites.

  Under *s 226 (2)* of the *Contract and Commercial Law Act 2017* where a signature is required by law (for example, is needed to create a binding agreement or verify the accuracy of information) the recipient must confirm that the use of an electronic signature is acceptable. This confirmation should be sought by the signatory prior to the electronic signature being used.

- Where an electronic signature is permitted and instruction is given to the signatory regarding using an electronic signature these should be followed by the signatory as much as practicable.

- When documents use an electronic signature and the document has a legal purpose, if sending electronically, where practicable the hard copy of the complete document with the hand written signature on the signature page should also be provided to the recipient.

- Under *s 228* of the *Contract and Commercial Act 2017* an electronic signature is presumed to be reliable and appropriate where certain conditions are met. To meet these conditions, staff should consider the following:

    - Storing master copies of an electronic signature in a password protected electronic folder, or in another secure place electronically**.**

    - Only those with specific authority from the signatory to use the signature on correspondence sent on the behalf of the signatory should have access to the password. Those with authority to use the signature to send out correspondence on behalf of the signatory should be clearly recorded on a "Signature Use" register and record when the signature was used.

    - If using an electronic signature for University business, University of Canterbury email addresses should only be used to send the signed correspondence or documents.

For Students

- Students wishing to submit work or applications via an electronic signature can only do so if permissible by the relevant authority/department/school or using an approved form that expressly allows the use of an electronic signature.

  Electronic signatures used by students should be cross-checked by staff against official University documents where the student has previously signed and those document have been accepted, or valid identification information where the signature has been used (passport or drivers licences).

UNIVERSITY OF CANTERBURY
Te Whare Wānanga o Waitaha
CHRISTCHURCH NEW ZEALAND

APPENDIX 2

Key Components of a Fraud Response Plan 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 Executive Director/Chief Financial Officer (CFO) will approve the plan.

2. The plan should consider any internal arrangements 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 Communications and External Relations 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 CFO.