Waimate District Council

FRAUD POLICY 311

TABLE OF CONTENTS

POLICY OVERVIEW

1.0 PURPOSE

1.1 To define internal controls, mechanisms, and systems as to minimise, detect, counter, and/or prosecute (if applicable) all instances of fraudulent activity by all parties employed by, elected to, contracted to, volunteering for, or service-recipient of, Waimate District Council (Council); and

1.2 To ensure that all such control systems are implemented consistently, impartially, systematically, and comprehensively; and

1.3 To formalise that in implementation of the present policy, Council shall:

a. recognise a zero tolerance policy towards any instance of fraud, and
b. collect and secure all evidence in support of prosecution, and
c. where appropriate, engage external forensic and enforcement agencies for the purpose of investigating and prosecuting any instance of fraud, and
d. pursue the recovery of any loss caused by fraudulent activity.

2.0 APPLICABILITY

2.1 The policy applies to all Council staff, elected members, and all consultants, vendors, contractors, volunteers, and agencies with business relationships with Council.

2.2 The policy does not apply to performance management issues deemed unrelated to fraud.

3.0 DEFINITIONS

3.1 For the purpose of the policy, the term 'fraud' encompasses a wide spectrum of unlawful activities that are intentionally perpetrated for illegitimate personal gain, including but not confined to acts of bribery,[1] corruption,[2] fraudulent financial reporting, embezzlement, deception, intellectual property theft, or any form of misappropriation of assets.

3.2 Within such a framework, activities that constitute fraud include, but are not limited to:

a. unauthorised or improper use of Council funds;
b. unauthorised use of Council facilities, vehicles, equipment, records, or intellectual property for personal gain;

---

[1] The term bribery defined as "an act of giving money or another item of value in exchange for an altered behaviour that benefits the giver", as outlined by, Audit New Zealand, 'Fraud' <https://www.auditnz.govt.nz/good-practice/csf/fraud> [accessed September 2019]

[2] The term corruption defined as "behaviour on the part of officials in the public or private sector in which they improperly and unlawfully enrich themselves or those close to them, or induce others to do so, by misusing the position in which they are placed", as outlined by, Serious Fraud Office, 'Serious Fraud and Corruption' <https://www.sfo.govt.nz/what-fraud-is-and-what-we-do> [accessed September 2019]

c. manipulation of reporting or records as to obscure impropriety;
d. taking or dealing, without proper authorisation, any funds belonging to Council;
e. conducting any digital/cyber activities via Council's digital devices for the purpose of altering, destroying, forging, or manipulating records or data for fraudulent purposes;
f. forgery or unauthorised alteration of Council documents and accounts;
g. disclosure of confidential or proprietorial information to third parties;
h. unauthorised acceptance of gifts or items of material value from parties such as consultants, vendors, or contractors without the specific consent of the Chief Executive;
i. unauthorised acceptance of any form of personal fee, reward, gift, gratuity, or subsidy- or any attempt to extract the same whether on account of any services provided in the normal course of duty or otherwise;
j. signing any document, or making any statement, on behalf of Council without authorisation;
k. falsification of Council's records or data;
l. exploitation of a position of employment or knowledge/insight obtained from such a position to obtain benefit, financial or otherwise, either for oneself or for a third party other than Council;
m. use of Council accounts, credit facilities, purchase card, or credit card for personal gain;
n. presenting false credentials or qualifications;
o. being accessory to acts of fraud perpetrated by others;
p. failure to inform Council as to the existence of an act of fraud perpetrated by another while having knowledge of such an act;
q. all forms of theft of time, such as falsification of timesheets;
r. false expense claims; and
s. unauthorised or inappropriate use of loyalty reward schemes.

4.0 RELEVANT LEGISLATION

4.1 Relevant legislation includes, but not confined to:

a. Crimes Act 1961
b. Employment Relations Act 2000
c. Local Government Act 2002
d. Privacy Act 1993
e. Protected Disclosures Act 2000

5.0 POLICY STATEMENT

5.1 Council utilises a 'zero tolerance' policy towards all fraudulent activities, and shall conduct systematic, methodical, and comprehensive investigation into all alleged acts of fraud. All such investigations shall be conducted in full compliance with the principles of confidentiality, objectivity, and impartiality.

5.2 Rights of implicated parties, during the conduct of an investigation, will be upheld at all times. In conduct of its investigation, Council shall uphold the principle of confidentiality for both the investigated party and the whistle-blower by protecting their identities, unless compelled otherwise in compliance with either the necessities of an investigation or to prevent harm to public health and safety or to the environment.

5.3 Specifically related to implicated parties in a fraud investigation, Council shall do its utmost to ensure that, in compliance with existing legislation and the confines of the current policy, the interest and reputation of such individuals are fully protected during an investigation process. Council shall treat, and protect, the interests and reputation of any investigated individual with highest sensitivity.

5.4 All participants in a fraud investigation process shall maintain complete confidentiality of all aspects of the investigation while such investigation is being conducted.

5.5 Staff members who intentionally and with malice of forethought make false allegations of fraud against another party will be dealt with in accordance with Council's disciplinary procedures, as outlined in the Waimate District Council Staff Manual.

5.6 The overall responsibility for all fraud-related matters is with the Chief Executive. If the Chief Executive is implicated, the responsibility is transferred to the Mayor. This principle applies to all segments related to the Chief Executive's responsibilities and functions throughout this document.

PROCEDURES

6.0 HIERARCHY OF RESPONSIBILITIES

THE CHIEF EXECUTIVE

6.1 The Chief Executive has the primary responsibility for presiding over all investigations into alleged/suspected acts of fraud. If the Chief Executive is implicated or is involved in any capacity, the Mayor assumes the responsibility for all ensuing investigations.

6.2 The Chief Executive may appoint an Investigating Officer (IO) at any stage of the investigation to oversee any case of alleged/suspected fraud on their behalf.

6.3 In the advent of discovery of fraud and prior to the conclusion of the initial enquiry, the Chief Executive is to notify the Mayor, the Audit & Risk Committee, the Human Resources Manager, and where appropriate, Council's insurers and/or Audit New Zealand.

6.4 During the course of an investigation, the Chief Executive is to inform the above stakeholders (where applicable) of all pertinent investigative findings.

6.5 The Chief Executive is responsible for all communications, whether internal or external, relating to any fraud investigation, past or present.

6.6 If it is established that an instance of fraud has occurred, the Chief Executive is then responsible for informing external forensic investigating agencies (e.g. New Zealand Police, Serious Fraud Office, Audit New Zealand, Council insurers, etc.), where appropriate.

FRAUD CONTROL OFFICER

6.7 A Fraud Control officer (FCO) is responsible for initiating an enquiry into any reports of fraudulent activity. Council's pre-designated FCOs are:

a. Asset Group Manager
b. Community & Strategy Group Manager
c. Regulatory & Compliance Group Manager

6.8 FCO shall immediately notify the Chief Executive of any reported allegation of fraud upon having received such a report. Subsequently, the Chief Executive shall assign one of the designated FCOs to conduct the initial enquiry as to primarily:

a. determine the credibility of the allegation/suspicion, and where applicable,
b. determine the degree of the allegedly committed fraud, and
c. identify and secure all relevant evidence.

INVESTIGATION OFFICER (IO)

6.9 With the conclusion of the 'initial enquiry' stage of an investigation, the IO is appointed by the Chief Executive to oversee next stages of the investigation.

6.10 The IO may be an FCO or another member of staff, or an external body, as deemed appropriate by the Chief Executive.

6.11 The IO is responsible for ensuring that all physical and/or electronic evidence is preserved in a safe place for future examination.

7.0 MECHANISM OF INFORMING THE FCO

7.1 All members of staff, elected members, consultants, contractors, vendors, and volunteers are obliged to report any instance of suspected fraud to any of the pre-designated FCOs immediately.

7.2 Any party reporting a suspected fraudulent activity must:

a. not contact the suspected individual in an effort to determine the facts or demand restitution;
b. not discuss the case facts, suspicions, or allegations with any parties external to Council (including the media) unless specifically instructed to do so by the Chief Executive;
c. not discuss the case with parties internal to Council other than the FCO, the IO, and/or the Chief Executive;
d. not deliberately make false allegations.

7.3 If 2 or all FCOs are implicated in any manner, the alleged/suspected fraud must be directly reported to the Chief Executive.

7.4 If the source of a report believes that it is not appropriate to inform any of the pre-designated FCOs, they may directly report to the Chief Executive.

7.5 The source of a report may select to remain anonymous, and instead submit the report in writing. Anonymous reports will be investigated as far as is reasonably practicable.

7.6 The FCO shall acknowledge all non-anonymous reports in writing. The source of a disclosure must be informed of any action or recommended action related to that disclosure within 20 working days after the date on which the disclosure was made.

7.7 Confidentiality must be maintained at all times, unless:

a. the source consents in writing to the disclosure of their identity; and/or

b. that investigating officers/agencies believe that disclosure of identifying information is paramount to the effective investigation of allegations cited in the protected disclosure, and/or
c. the breach of confidentiality is essential to prevent serious risk to public health and safety, and/or to the environment, and/or
d. that, having regard to the principles of natural justice, it is deemed essential.

8.0 INVESTIGATION PROCESS

INITIAL ENQUIRY

8.1 There are 5 purposes to the initial enquiry, an enquiry that constitutes the first stage of the investigation process, as outlined below:
a. to establish the credibility of the suspicion/allegation; and
b. to conduct a preliminary assessment as to determine whether the reported instance is caused by either mistake or by design (i.e. to establish intention); and
c. to identify all relevant evidence, and to secure all such evidence; and
d. If applicable, identify mitigation measures as to prevent ongoing or future fraud, and
e. to inform the Chief Executive accordingly.

8.2 Investigative steps usually associated with the initial enquiry stage are steps such as enquiries of staff, review of documents and records, and interrogation of computer systems, *inter alia*. The FCO shall analyse all evidence, and pursue all relevant leads, exhaustively, regardless of whether an instance is caused by either error or intention.

8.3 The FCO shall conduct the investigation with complete impartiality and neutrality, with no regard for the involved parties' position within the Council's organisational structure, or their relationship with Council, or their length of employment.

8.4 The FCO shall only investigate matters that are the subject of, or related to, the suspected fraud.

PREVENTION OF FURTHER LOSS

8.5 Member(s) of staff suspected of fraud may be suspended, with pay, pending the outcome of the investigation. In such circumstances, the IO may request that the suspended party is:
a. approached unannounced;
b. supervised at all times before leaving Council premises;
c. prevented from removing any property belonging to Council;
d. instructed to return all Council IT equipment (e.g. tablets, phones, etc.),
e. to surrender any security passes and/or keys to the premises, for which the appropriate receipt shall be issued and endorsed by the suspended party.

8.6 If suspension is imposed, the Corporate Services Group Manager shall advise as to the best method of preventing the suspended party's future access to Council facilities for the duration of their suspension.

8.7 If suspension is imposed, the Senior Network Administrator may be requested by the IO to withdraw the suspended party's access permissions to Council's computer systems and all related digital domains and networks.

8.8 The IO is to ensure that all steps for securing evidence and prevention of further loss are undertaken, as outlined in 'Appendix 1: Securing Evidence Checklist' (See Appendix 1).

POTENTIAL OUTCOMES OF AN INITIAL ENQUIRY

8.9 By its conclusion, the initial enquiry shall yield one of the following outcomes:

a. If no fraud detected, then the investigation shall be terminated. If the FCO, reporting to the Chief Executive, establishes that there is no credible substance to the suspicion/allegation, then the investigation process is terminated and the outcome is advised in writing to the source making the allegation.

b. If fraud detected, then upon receiving the FCO's report, the Chief Executive shall first notify the Mayor, the Audit & Risk Committee, and the Human Resources Manager (i.e. the internal stakeholders). Where appropriate, the Chief Executive is to inform Audit New Zealand and Council's insurers (i.e. the external stakeholders). The Chief Executive shall then determine whether to engage external forensic agencies (e.g. New Zealand Police, Serious Fraud Office, etc.). If external forensic agencies are engaged, all secured documents, records, and all such physical/electronic evidence, shall be transferred to such investigating parties. Copies of all original documents, records, and all such evidence must be kept by Council as transferred original documents may not be returned to Council. The outcome is advised in writing to the source making the allegation.

INITIAL ENQUIRY REPORT

8.10 At the conclusion of the initial enquiry stage of the investigation, a written report will be prepared by the FCO, outlining the facts discovered by the investigation. Such report shall include reference(s) to supporting evidence, and copies of such evidence ought to be attached to the report.

8.11 The initial enquiry report will not be disclosed to, or discussed with, anyone other than the person making the allegation and those who have a legitimate need to know (e.g. the Mayor, and the Audit & Risk Committee, etc.). Limited and controlled circulation of the investigation report is essential to avoiding damaging the reputation of those parties previously suspected of fraud but subsequently found to be innocent of any wrongful conduct, and to protect Council from potential liability.

8.12 The report shall contain:

a. description of the incident, including the amount of any loss;
b. identification of parties involved;
c. description of the means of, and methods used for, perpetuating the fraud;
d. assessment of reputational impact;
e. assessment of communications;

f. if applicable, recommendation on measures required to prevent recurrence; and
g. if applicable, recommendation on methods to strengthen future responses.

8.13 The report shall not include:
a. any statements that cannot be supported by facts;
b. any judgement on guilt or innocence of parties named in the report;
c. any prejudgement on the outcome of any possible disciplinary hearing, civil recovery action, or criminal prosecution.

8.14 If deemed appropriate by the Chief Executive, Council staff shall be briefed upon the conclusion of the investigation.

9.0 CONFIDENTIALITY AND MEDIA

9.1 Subject to legal requirements or necessities of an investigation, all disclosed information by any parties involved in either a formal investigation or an informal process must be kept confidential.

9.2 It is the responsibility of the IO to outline the limits of confidentiality to parties involved in an investigation, as outlined in the Waimate District Council Protected Disclosure Policy.

9.3 Notwithstanding the above, if an instance of fraud is discovered/substantiated, Council reserves the right to share necessary information with Audit & Risk Committee, elected members, New Zealand Police, Serious Fraud Office, Audit New Zealand, Council's insurers, or any external forensic investigative agency deemed appropriate by the Chief Executive.

9.4 The Chief Executive has overall responsibility for leading and coordinating all communication both internally and externally on all fraud-related matters.

9.5 All staff are required to direct any media communication, or media requests for information or comments, or any other requests for information from either internal or external parties, to the Chief Executive. Staff must refrain from providing any comment on fraud-related matters, whether past or present, to any parties either internal or external to Council.

10.0 FRAUD PREVENTION AND MINIMISATION

10.1 Council is committed to the development and maintenance of best procedures for detecting, preventing, or minimising fraud. This primarily means the implementation and controlled operation of internal control systems, as outlined below.

10.2 The Human Resources Manager is responsible for:
a. ensuring appropriate pre-employment reference and qualification checks are carried out. Credit and criminal record checks can be carried out if necessary;
b. overseeing induction procedures for new staff that include fraud awareness, protected disclosure awareness, and Code of Conduct training;
c. ensuring that staff appointed to positions of responsibility are appropriately qualified, experienced, and aware of their obligations in regard to fraud and the protection of Council assets;

d. ensuring all staff are aware of, and have access to, the Protected Disclosure Policy.

10.3 The Corporate Services Group Manager is responsible for:

a. Arranging regular fraud awareness training for all Council staff in general, and for FCOs in particular.

10.4 The following internal audit procedures are to be systematically observed in order to detect and deter fraud:

a. two authorisations required on all bank transactions made;
b. two authorisations required on all invoices raised;
c. daily general ledger controls to be conducted (automatically emailed to the accountant overnight);
d. fortnightly Datacom wages maintenance schedules to be checked and signed off by the Corporate Services Group Manager, and in their absence, by the Accountant;
e. masterfile changes to be printed out daily and signed off by the Corporate Services Team Leader;
f. any changes made to the daily general ledger masterfile to be checked and signed off by Corporate Services Group Manager;
g. monthly reconciliations of suspense accounts to be reviewed by the Accountant or the Corporate Services Group Manager;
h. daily review of bank reconciliations to be undertaken;
i. due diligence checks on suppliers to be conducted;
j. the Corporate Services Team Leader to maintain a file holding supporting documentation for creditors bank account numbers to ensure the correct accounts are being credited. These are to be inspected periodically and randomly for anomalies;
k. the staff debtors and fuel accounts to be monitored by the Accounts Receivable Officer for deficits and excessive credits (i.e. over $500.00);
l. the Human Resources Manager to monitor leave balances to ensure no staff member is accumulating excessive leave without explanation;
m. annual stocktakes to be conducted.

11.0 DOCUMENT CONTROL

Queries:	Corporate Services Group Manager
Effective:	8 October 2019
Previous Review Date(s):	2 August 2016
Next Review Date:	8 October 2022
Document Owner:	Corporate Services Group Manager
To be only amended by:	Resolution of Council

Approved by: _____ Date: 8 October 2019

Stuart Duncan, Chief Executive

APPENDIX 1: SECURING EVIDENCE CHECKLIST

Sources of electronic evidence include:		Steps to secure records
• any computer or tablet device used by relevant staff • mobile phones	☐ ☐	Turn off, label, physically secure and do not allow any staff to access or use until they can be forensically copied.
• Current mailbox or email servers • current contents of network home directories and shared group drives • internet and printer logs for the relevant period;	☐ ☐ ☐	Ensure IT staff preserve such data, and do not allow any user to access this data until it can be forensically copied. All logins belonging to the investigated parties to be disabled.
• backup or disks containing user data such as email, user home directories or shared group directories	☐	Label and remove backup from the backup cycle (e.g. replace with new blank tapes) to ensure potentially relevant backups are not overwritten.
• removable hard drives or USB memory sticks	☐	Physically secure, label, and do not allow staff to access or use until they can be forensically copied.
• building access records (swipe card logs) • CCTV footage • electronic phone records from PABX or mobile service provider	☐ ☐ ☐	Secure the records and ensure they are not overwritten or deleted.
Sources of physical evidence include:		**Steps to secure records**
• employee's office, desk, locker, or other storage areas • filing cabinets, either personal, group, or project specific	☐ ☐	Physically secure until they can be properly searched
• related employee records: Human Resources file, performance reviews, employee contract, relevant policies and procedures, address book, diary, business card holders • financial records: itemised telephone billing records (landline and mobile), credit card billing records • related expenses, payments, and other financial data	☐ ☐ ☐	Contact relevant business functions and advise to secure records and provide verified copies
Considerations when securing evidence:		
• Prevent staff access to evidence in order to help maintain its integrity • Secure all evidence to maximise its evidentiary value • A sound forensic approach will support the provision of independent expert evidence, if required • In cases where a user's access should be removed, the IO should consider all possible access points, including physical access and remote access through computers, telephones, and other digital devices		
Considerations before evidence:		
• make sure you review relevant Council policies, employee contracts, and relevant legislation, regarding privacy, confidentiality and surveillance issues		