

ELECTORAL OFFICE FOR NORTHERN IRELAND



FRAUD POLICY & RESPONSE PLAN

Issue Date – 30 January 2007

FRAUD POLICY & RESPONSE PLAN



1	INTRODUCTION	2
2.	EONI POLICY	3
3.	PREVENTION AND DETECTION MEASURES	3
4	WHEN FRAUD IS SUSPECTED OR DETECTED	6
5	THE RESPONSE PLAN	6
	• Introduction	6
	• Dealing with suspected fraud	7
	• Reporting a suspected fraud	7
	• Suspected fraud formally reported to the Chief Electoral Officer	8
	• Managing the fraud investigation	9
	• Outcome of fraud investigation	11
6.	CONCLUSION	12
	Annexes	
	Annex A Further Information	14
	Annex B The Seven Principles of Public Life	15
	Annex C Definitions	17
	Annex D Identifying and dealing with the risk of fraud	19

1. **INTRODUCTION**

This document is for use by the Electoral Office for Northern Ireland staff and those directly involved in managing the risk of fraud. It provides the framework for prevention, detection, and response to fraud and other offences of dishonesty including theft and corruption.

- 1.1. This policy and plan applies to all frauds committed within the Electoral Office for Northern Ireland [EONI]. The policy and plan can be accessed by staff in the Common Folder. A very simple definition of fraud is – “a false pretence intended to have a practical result.” So, for example, deliberately mis-stating the mileage claimed on an expenses form would be fraud even if the amount improperly claimed is very small. Similarly, even very small mis-statements on a flexi sheet are fraudulent if they are deliberate. The policy also applies to other acts of dishonesty such as franking personal mail or taking home for personal use pens or other stationery items. Both of these amount to theft.
- 1.2. EONI already has comprehensive procedures in place that reduce the likelihood of fraud occurring. These include Risk Management arrangements, documented financial policies and procedures, and a system of internal controls. EONI also tries to ensure that a risk (and fraud) awareness culture exists throughout the organisation. This is built into the annual Business Plan.
- 1.3. Should these internal controls fail and a fraud is suspected or detected, then Chapter 5 sets out the formal response plan for dealing with such incidents.
- 1.4. The integrity and honesty of EONI staff is critical to the effective operation of the office. Fraud and other acts of dishonesty committed by an individual member of staff call into question the integrity and honesty of the whole organisation. All acts of fraud and dishonesty that are proved will be treated very seriously. Each case will be treated on its individual merits but, in the absence of exceptional

mitigating circumstances, such actions are likely to be regarded as gross misconduct.

Annex A provides sources of further advice and information on various aspects and the implications of the fraud management process.

1.5 This Fraud Policy and Response Plan were adopted by EONI Management Board on 17 August 2006 and will come into effect immediately.

1.6 This Fraud Policy and Response Plan will be subject to a formal review two years after it comes into effect or earlier if required.

2. **EONI POLICY**

EONI is committed to maintaining an open environment to fulfill the objectives of the organisation. It is also committed to the elimination of any fraud and to ensuring that wrongdoers are dealt with appropriately. The progress of a case through the police and prosecution systems will not be a limiting factor on the organisation's ability to take action against staff where they are found guilty of misconduct through the relevant internal disciplinary procedures. EONI will take proportionate steps to recover any losses incurred as a result of fraud, corruption or theft.

2.1. EONI wishes to encourage anyone having reasonable suspicions of fraud to report them. It is also EONI policy that no one will suffer in any way as a result of reporting a reasonably held suspicion. For these purposes "reasonably held suspicions" shall mean any suspicions other than those which are groundless and/or raised maliciously.

2.2. The Chief Electoral Officer (CEO) is ultimately responsible for establishing the internal control system designed to counter the risks the organisation faces. He is accountable for the adequacy and effectiveness of these arrangements. Managing fraud risk is seen by EONI in the context of managing a wider range of risks. EONI promotes an anti-fraud culture by encouraging management to create conditions in which staff have neither the motivation nor the opportunity to commit fraud.

3. **PREVENTION AND DETECTION MEASURES**

When risks and deficiencies in the level of control are identified, it is necessary to choose the most appropriate and proportionate type of controls [a huge security system is not required to prevent minor acts of fraud]. Prevention is always preferable to detection. Strong prevention controls exist wherever possible. As prevention controls may not be sufficient to guard against determined fraudsters, detection controls are also important. Detection controls are established to detect errors,

omissions and fraud after the events have taken place. The range of controls put in place by are detailed below.

- 3.1. **Physical security:** This is a prevention measure with controls to monitor access to documentation, IT systems or assets ensuring that there is no unauthorised use, loss or damage. Assets can range from computer terminals on desks, to cheques sent out to pay suppliers.
- 3.2. **All assets** are held securely, and access to them restricted as appropriate. This control applies not only to the premises, but also to computers, databases, banking facilities, documents and any other areas critical to the operation of EONI. It may even be appropriate to restrict knowledge of the existence of some assets. This decision is reserved for the Chief Electoral Officer.
- 3.3. **Access to computer systems** is an important area which is very tightly controlled, not only to prevent unauthorised access and use, but also to protect the integrity of the data. The Data Protection Act requires computer and data owners to secure information held on their systems which concerns third parties. The threat to computers can come from both inside and outside an organisation as computer hackers may gain access in order to extract or corrupt information. The computer itself is also vulnerable to theft, both in terms of hardware and software. This type of theft has the additional cost of potential major disruption to the core operations of the organisation.
- 3.4. **Segregation of Duties** to avoid conflicts of interest or opportunities for abuse is standard practice throughout EONI. This is also largely a preventive measure ensuring that the key functions and controls over a process are not all carried out by the same member of staff, e.g. ordering goods should be kept separate from receipt of goods; similarly authorisation and payment of invoices; thus avoiding undue reliance on any one individual.

- 3.5. **Supervision and checking of outputs:** This includes monitoring work methods and outputs of staff to ensure controls are effective. This is both a preventive and detection control.
- 3.6. **Audit trail:** This is largely a detective control although its very presence can have a preventive effect.
- 3.7. **Monitoring:** EONI's management operates a policy of random checks in potential risk areas to ensure controls are operating effectively and promote management's commitment to the prevention of fraud and corruption.
- 3.8. **Evaluation:** EONI will periodically review processes to improve their effectiveness and tighten controls. This evaluation will from time to time be done by internal audit.
- 3.9. **Asset accounting:** EONI operate a fixed asset register and has an inventory of all capital assets e.g. computers.
- 3.10. **Budgetary and other financial controls:** A system of devolved budgets and delegated limits is used to ensure expenditure is properly approved and accounted for in line with the HM Treasury's guide on regularity and propriety.
- 3.11. **Fraud indicators – warning signs**
Managers should also be alert to any warning signs that might indicate that fraud is taking place. These may include:
- Staff under stress without a high workload
 - Always working late
 - Reluctance to take leave
 - Reluctance or refusal to transfer
 - Refusal of promotion
 - Unexplained wealth
 - Sudden change of lifestyle
 - New staff resigning quickly

- Cosy relationships with suppliers/contractors
- Suppliers/contractors who insist on dealing with one particular member of staff.

4. **WHEN FRAUD IS SUSPECTED OR DETECTED**

EONI requires all staff at all times to act in accordance with the seven principles of public life, as set out in Annex B. This includes safeguarding the public resources for which they are responsible. EONI will not accept any level of fraud or corruption; all cases will be thoroughly investigated and dealt with appropriately. EONI is committed to ensuring that opportunities for fraud and corruption are reduced to the lowest possible level.

4.1. In the event that a fraud comes to light, staff are advised to report it urgently as described in the guidance issued in Guidance to Staff on Fraud EONI 2007 (Version1) which can be accessed in the Common Folder and Fraud Awareness Leaflet EONI 2007 (Version 1), issued to staff in January 2007.

4.2. There are four main ways in which fraud or corruption comes to light:

- Management controls being broken, or management suspicions;
- Routine audit engagements or specific audit checks on high risk areas;
- A "tip-off" from a third party, either internal staff or external staff or
- By chance.

5. **THE RESPONSE PLAN**

5.1. **Introduction**

This plan sets out EONI's response to a detected or suspected fraud. For simplicity the document will use the term "fraud" to cover a range of circumstances (including theft, loss, misappropriation and wilful damage) although it is recognised that each may have a separate legal definition.

5.1.1. The plan provides guidance and procedures to ensure that evidence gathered is admissible in any further criminal, civil or disciplinary action. This guidance will need careful consideration in relation to the actual circumstances of each case

before action is taken. It is emphasised that this document is not intended to provide direction on the prevention of fraud, which is largely addressed through the internal control system.

5.2. **Dealing with suspected fraud**

5.2.1. EONI undertakes to deal with all matters in confidence and in strict accordance within the terms of the Public Interest Disclosure Act 1998. This statute protects the legitimate personal interests of staff. Vigorous and prompt investigations will be carried out into cases of actual or suspected fraud as appropriate.

5.2.2. **Reporting a suspected fraud**

A member of staff having reasonable suspicions that a fraud is taking place within the organisation should immediately inform his/her line manager. The line manager should discuss the nature of the suspicions with the informing member of staff before notifying the Chief Electoral Officer. If the member of staff believes that the line manager is involved in the fraud it should be reported direct to the Chief Electoral Officer.

5.2.2.1. Considerable care needs to be taken to ensure nothing is done to prejudice a fair investigation or give rise to an action for slander or libel. Staff are strongly advised to exercise caution at all times when dealing with accusations of fraud. The manager should take no further action without first informing the Chief Electoral Officer.

5.2.2.2. If the line manager appears to be blocking the progress of an investigation, the individual should report suspicions directly to the Chief Electoral Officer. If the Chief Electoral Officer is suspected this should be reported to the Political Director at the NIO.

5.2.3. **Suspected fraud formally reported to the Chief Electoral Officer**

The CEO will treat all reported suspicions as serious, and respond faithfully to concerns raised by staff. Although responsibility for the investigation rests on him, he will normally delegate the task to the Assistant Chief Electoral Officer.

- 5.2.3.1. The first response of the Assistant Chief Electoral Officer to any allegation of suspected fraud must be to determine whether there is any substance to the allegation. She must consider if prompt action is needed to prevent further loss, and where appropriate, protect any evidence that demonstrates a fraud has occurred.
- 5.2.3.2. Line Managers must immediately record all reported suspicions in a log, including those dismissed as minor or otherwise not investigated. The log will be retained confidentially by the Head of Corporate Services, available to the Chief Electoral Officer as accounting officer, to internal and external audit and the Management Board. The log will contain details of actions taken and conclusions reached.
- 5.2.3.3. Where there are grounds for believing that a criminal offence has been committed, all the facts should be reported to the police without delay. Reporting the suspicion to the PSNI should not be delayed because some of the facts are not yet known. 'If in doubt report to the PSNI.' In certain circumstances, the police may recommend that there be no further disclosure or investigation by EONI staff, in case such action compromises a future criminal investigation [including taking action to stop a loss or tighten controls or precautionary disciplinary suspension].
- 5.2.3.4. The Chief Electoral Officer must advise the Head of Elections Unit, Rights and International Relations Division, Northern Ireland Office if he has decided to suspend a member of staff or if he believes there has been a significant loss.
- 5.2.3.5. When an allegation of suspected fraud is first made known to the Chief Electoral Officer, he will normally inform the subject of the allegation without undue delay (unless advised otherwise by the police, or where covert surveillance is required, in order not to prejudice the prevention or detection of a fraud). The individual normally is entitled to know the nature and source of the allegation. He/she should be advised that the CEO will be undertaking a formal investigation in accordance with the organisation's Fraud Response Plan, and under the authority of the relevant disciplinary procedure. He/she should also be informed

that they will be entitled to representation as allegations are presented, during the investigation, and at any subsequent disciplinary hearing.

5.2.3.6. The Chief Electoral Officer remains responsible for the effective management of the investigation. Where he has delegated this function to the Assistant Chief Electoral Officer he must agree the investigation objectives, parameters, resources and reporting mechanisms with her and see to it that she -

- Notifies EONI's internal auditors
- Advises the Head of Elections Unit, Rights & International Relations Division where the incident is likely to result in adverse publicity.
- Consults with the PSNI where necessary.
- Prepares the final investigation report, consider the evidence obtained and confirm the recommendation reached.
- Considers the possibility of recovering losses through the application of civil action.

5.2.4. **Managing the Investigation.**

The following is intended to be general guidance to assist management in deciding the best course of action.

5.2.4.1. **Diary of events**

The Chief Electoral Officer or Assistant Chief Electoral Officer will keep a Diary of Events to record the progress of the investigation.

5.2.4.2. **Does it appear a criminal act has taken place?**

Consideration should be given to whether a criminal act has taken place. In practice it may not be completely clear whether a criminal act has taken place. If a criminal act is suspected, the police should be informed.

5.2.4.3. **Covert surveillance**

There may be exceptional circumstances where it is considered necessary to conduct covert surveillance of an individual in order not to prejudice the prevention or detection of a fraud. The Chief Electoral Officer has very limited

authority to conduct such surveillance and it will only be undertaken in liaison with the PSNI.

5.2.4.4. Witnesses/interview procedure

Where appropriate the Assistant Chief Electoral Officer should take written statements from witnesses. The witness must sign the document as a true record. In taking the witness statements and conducting interviews regard will be paid to the requirements set out in the Police and Criminal Evidence (NI) Order 1989 [PACE].

Failure to comply with these procedures can prejudice the outcome of any disciplinary action or criminal proceedings. Advice on disciplinary procedures may be sought from the Human Resources Officer. The Chief Electoral Officer may provide advice on the PACE requirements.

5.2.4.5. Physical evidence

Upon taking control of any physical evidence, it is very important that a record is made of the time and place it is taken. If evidence consists of several items, for example many documents, each one should be tagged with a reference number corresponding to the written record. If documents are in a file, the whole file should be taken as evidence. Under no circumstances should the relevant documents be taken out of the file.

5.2.4.6. Unless otherwise advised by the police, the internal investigation will continue to determine the facts and recommend what if any disciplinary action is needed, what can be done to recover a loss and what may need to be done to improve internal control to prevent the event happening again.

5.2.4.7. All information and action taken should be carefully documented and held in a file which is given the appropriate protective marking [normally Restricted]. This file may be required as admissible evidence should disciplinary or police action be subsequently required. At all stages of the investigation care must be taken to act with tact and discretion as an unfounded allegation if handled incorrectly,

could damage the reputation of an innocent employee. The enquiry should therefore be carried out in strict confidence.

5.2.5. **Outcome of fraud investigation**

The Assistant Chief Electoral Officer will present the investigation report for consideration by the Chief Electoral Officer. The report will include -

- A summary of the investigation
- All statements taken
- Any exhibits taken
- A recommendation as to the action required

The updated fraud log shall be attached to the report.

5.2.5.1 **Recommendation**

The recommendation will be either that there is no case to answer and that no disciplinary investigation should be initiated, or that there is a case to answer and that a disciplinary investigation should be initiated. The Disciplinary Procedures issued in September 1994 are to be followed in any disciplinary action taken. This may involve a disciplinary hearing to determine the facts.

5.2.5.2 **Review events with Police**

Where relevant, evidence of fraud or another criminal offence should be reviewed with the police.

5.2.5.3 **Precautionary suspension**

The Chief Electoral Officer will decide whether or not to suspend the suspected member of staff, normally on full pay, as a precautionary measure pending the outcome of disciplinary / dismissal action.

5.2.5.4 **Recovery action** The Chief Electoral Officer will consider what can be done to recover any loss and whether anything should be done to improve control to prevent the event happening again.

5.2.5.5 **Losses and compensations register**

Guidance on losses and special payments is provided in Government Accounting issued by HM Treasury and will be followed if losses occur.

5.2.5.6 **Insurance**

The possibilities of recovering a loss through insurance, where appropriate, should not be overlooked.

6. **Conclusion**

This policy document provides the framework for preventing, detecting and responding to suspected or detected fraud and other offences of dishonesty.

- 6.1. It is recognised that the effectiveness of the control framework depends on the co-operation of all staff. Every individual is expected to act in accordance with the public service values set out in Annex B – the seven principles of public life. Individuals are encouraged to be vigilant and report any failures in the control framework at the earliest opportunity in order to reduce the potential for fraud.

Signed: Douglas Bain CBE TD Advocate
Chief Electoral Officer for NI

Dated: 30 January 2007

NIPSA has been consulted on this document and has provided a number of suggested amendments which have, in the main, been accepted by Management. Unfortunately however NIPSA is unable to sign the policy document due to a difference of opinion on one area, namely the area of a very tight definition of fraud and automatic linkage with a likely charge of gross misconduct (see paragraph 1.4), particularly in relation to flexi abuse. Whilst NIPSA fully accepts that flexi abuse is unacceptable and where discovered should warrant consideration of a penalty, NIPSA does not accept that this should be treated in the same way as actual physical theft or corruption, and certainly not on the first occasion. For example the usual penalty in the NICS for a first offence of this nature would be to remove the offending member of staff from the flexi scheme for a set period. Thereafter subsequent abuses may well be treated more harshly.

Further Information

Further information and guidance to supplement this document is available from the following sources:

- Management of Risk – A Strategic Overview (HM Treasury 2004) “The Orange Book”
- The Treasury’s “Managing the Risk of Fraud – A Guide for Managers” May 2003

Anyone involved in Detection and Prevention of Fraud Processes is encouraged to read the above documents which may be found on the Treasury Website.

<http://www.hm-treasury.gov.uk/>

The Seven Principles of Public Life

The seven principles below were identified in the Nolan report and should be the hallmark of all public servants behaviour.

1. **Selflessness**

Holders of public office should take decisions solely in terms of the public interest. They should not do so in order to gain financial or other material benefits for themselves, their family, or their friends.

2. **Integrity**

Holders of public office should not place themselves under any financial or other obligation to outside individuals or organisations that might influence them in the performance of their official duties.

3. **Objectivity**

In carrying out public business, including making public appointments, or recommending individuals for rewards and benefits, holders of public office should make choices on merit.

4. **Accountability**

Holders of public office are accountable for their decisions and actions to the public and must submit themselves to whatever scrutiny is appropriate to their office.

5. **Openness**

Holders of public office should be as open as possible about all the decisions and actions that they take. They should give reasons for their decisions and restrict information only when the wider public interest clearly demands it.

6. **Honesty**

Holders of public office have a duty to declare any private interests relating to

their public duties and to take steps to resolve any conflicts arising in a way that protects the public interest.

7. **Leadership**

Holders of public office should promote and support these principles by leadership and example.

All those who work in the organisation should be aware of and act in accordance with, these principles.

Definitions

There is currently no precise legal definition of fraud. The Theft Act (NI) 1969 covers many of the offences referred to as fraud. The term is used to describe such acts as deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts and collusion.

For the purposes of reporting fraud to the Treasury the following crimes fall within the context of the Fraud Report

1. **Theft**

Dishonestly appropriating the property of another with the intention of permanently depriving them of it (Theft Act (NI) 1969). This may include the removal or misuse of funds, assets or cash.

2. **False Accounting**

Dishonestly destroying defacing concealing or falsifying any account, record or document required for any accounting purpose, with a view to personal gain or gain for another, or with intent to cause loss to another or furnishing information which is or may be misleading, false or deceptive (Theft Act (NI) 1969).

3. **Bribery**

Any circumstances where an inducement or reward is offered or given which may influence the actions of others (Audit Commission).

4. **Corruption**

The offering, giving, soliciting or acceptance of an inducement or reward which may influence the actions taken by the authority, its members or officers (Public Bodies Corrupt Procedures Act 1889 and the Prevention of Corruption Acts 1906 and 1916).

5. **Deception**

An act of hiding the truth, especially to get an advantage – Theft Act (NI) 1969.

6. **Collusion**

Secret agreement or co-operation especially for an illegal or deceitful purpose (source: Merriam Webster's Collegiate Dictionary).

Identifying and dealing with the risk of fraud

Managing the risk of fraud is the same in principle as managing any other business risk. It is best approached systematically both at the organisational level e.g. by using fraud policy statements and personnel policies, and at the operational level. When considering fraud risks in specific operations there are a number of steps, which should be taken.

1. Identify risk areas

Establishing the areas most vulnerable to the fraud risk is done periodically through the internal and external audit review process. Patterns of loss and areas of potential loss should be identified so that vulnerable areas can be pinpointed. It may be useful to survey the staff involved in operating the system to establish all the risks of which they are aware. Areas where risks may be particularly high include those where there is responsibility for getting or managing contracts, handling cash and other assets, overtime and travel expense claims.

2. Assess scale of the risk

Identify and assess what measures are already in place to prevent fraud and determine the level of residual risk. This is done periodically as part of the financial procedures' review and audit planning process.

3. Allocate responsibility for risk

Responsibility for the management of each risk is allocated to relevant officers at the appropriate level in the relevant business plan.

4. Identify need for revised controls

Evaluation of the adequacy of existing controls and establishment of what further controls or changes to existing controls are required to reduce or eliminate the risk.

5. **Implement the revised controls**

The relevant Director will implement the necessary controls, liaising with internal audit as necessary.

6. **Monitor implementation of controls**

This is achieved by a number of means including internal audit reviews of system controls and spot checks by managers to ensure that controls such as supervisory controls or reconciliations, are in operation.

7. **Evaluate the effectiveness of controls**

Assessment of whether the risk of fraud is lessened as a result of the implementation of the revised controls will be based on audit opinion and management reviews.