##

**Finance Manual:**

**Section 8 Fraud and Bribery**

**The Police Rehabilitation**

**and Retraining Trust**

**Version 2.0**

**Date 31/10/2015**

# DOCUMENT CONTROL

|  |
| --- |
| Document History |
| **Version** | **Date** | **Owner** | **Changes** |
| 2 | 31/10/2015 | Finance Manager |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Release | Name | Approved / Comments | Date |
| Draft Check |  |  |  |
| HOD Approval | U Buchanan | Approved | 31 Oct 2015 |
| CEO Approval |  |  |  |
| BOD Approval |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |
| --- |
| Links and Dependencies |
| Section 1Finance Manual: IntroductionSection 2 Finance Manual: Payments (incorporating salaries)Section 3 Finance Manual: IncomeSection 4 Finance Manual: BankingSection 5 Finance Manual: Travel and SubsistenceSection 6 Finance Manual: Purchasing and ProcurementSection 7 Finance Manual: Gifts and Hospitality Section 9 Finance Manual: Conflicts of Interest |

CONTENTS

[DOCUMENT CONTROL 2](#_Toc443556407)

[1. Introduction 4](#_Toc443556408)

[2. What is Fraud? 4](#_Toc443556409)

[3. What is Bribery? 4](#_Toc443556410)

[4. Responsibilities 5](#_Toc443556411)

[4.1 Accounting Officer 5](#_Toc443556412)

[4.2 Head of Finance and Shared Services 6](#_Toc443556413)

[4.3 Managers 6](#_Toc443556414)

[5. Individual staff 6](#_Toc443556415)

[6. What to do if you wish to report a fraud? 7](#_Toc443556416)

[7. Conclusion 7](#_Toc443556417)

[Appendix A - Fraud Response Plan 8](#_Toc443556418)

# 1. Introduction

The Finance Manual consists of 9 sections which are listed below and you can find a separate policy document on the intranet for each one. This document is Section 8 – Fraud and Bribery Policy.

1. Introduction
2. Payments (incorporating salaries)
3. Income
4. Banking (incorporating credit card)
5. Travel and Subsistence
6. Purchasing and Procurement
7. Gifts and Hospitality
8. Fraud and Bribery Policy (incorporating Fraud Response Plan)
9. Conflicts of Interest

There is a continuing need to raise awareness of the responsibility of staff at all levels to safeguard public resources against the risk of fraud. The overall purpose of this Anti-Fraud Policy is to detail responsibilities regarding the prevention of fraud. The procedures to be followed in the event of a fraud being detected or suspected are detailed in the Fraud Response Plan (Appendix A attached).

The Police Rehabilitation and Retraining Trust (PRRT) require all staff, at all times, to act honestly and with integrity, and to safeguard the public resources for which they are responsible. Fraud is an ever-present threat to these resources and must be a concern to all members of staff. PRRT will not accept any level of fraud or corruption; consequently, any case will be thoroughly investigated and dealt with appropriately. PRRT is also committed to ensuring that opportunities for fraud and corruption are minimised.

# 2. What is Fraud?

Prior to the Fraud Act 2006 becoming law in Northern Ireland in January 2007, there was no precise legal definition of the term “fraud”. The Fraud Act, however, created a new general offence of fraud and indicated that fraud could be committed in three ways – by false representation; by failure to disclose information; and by abuse of position.

This Anti-Fraud Policy essentially covers fraud in its widest sense, and as such it covers cases of theft, false accounting, bribery and corruption, conspiracy to defraud, money laundering, forgery, extortion, embezzlement, misappropriation, concealment of material facts and collusion etc.

# 3. What is Bribery?

The Bribery Act 2010 came into effect on 1 July 2011. It defines four new criminal offences of offering or paying a bribe; requesting or receiving a bribe; bribing a foreign public official; and failure of commercial organisations to prevent bribery by persons associated with them.

This Policy is concerned with occupational fraud and bribery i.e. fraud committed by employees or contractors/associates of PRRT in the course of their work.

Occupational fraud, bribery and abuses fall into four main categories:

* theft, the misappropriation or misuse of assets for personal benefit;
* bribery and corruption;
* false accounting and/or making fraudulent statements with a view to personal gain or gain for another: for example falsely claiming overtime, travel and subsistence, sick leave or special leave (with or without pay);
* externally perpetrated fraud against an organisation.

Concerns which should be reported include, but are not limited to, staff committing or attempting to commit:

* any dishonest or fraudulent act;
* forgery or alteration of documents or accounts;
* misappropriation of funds, supplies or other assets;
* impropriety in the handling or reporting of money or financial transactions;
* profiting from an official position;
* disclosure of official activities or information for advantage;
* accepting or seeking value from third parties by virtue of official position or duties;
* theft or misuse of property, facilities or services.
* Accepts bribes or offering bribes.

External organisations’ or those of associates which should be reported include:

* being offered a bribe or inducement by a supplier;
* receiving fraudulent (rather than erroneous) invoices from a supplier;
* reported allegations of corruption or deception by a supplier.

# 4. Responsibilities

Annex 4.7 of Managing Public Money in Northern Ireland sets out the general responsibilities of public sector organisations in relation to fraud.

## 4.1 Accounting Officer

The Accounting Officer is responsible for establishing and maintaining a sound system of internal control that supports the achievement of PRRT’s policies, aims and objectives. The system of internal control is designed to respond to and manage the whole range of risks that PRRT faces. Managing fraud and bribery risks should be seen in the context of the management of this wider range of risks.

## 4.2 Head of Finance and Shared Services

The Head of Finance and Shared Services is responsible at an operational level for managing the risk of fraud, and as such will:

* develop and maintain effective controls to prevent fraud and bribery;
* ensure that if fraud or bribery occurs a vigorous and prompt investigation takes place;
* take appropriate disciplinary and legal action in all cases, where justified;
* review systems and procedures to prevent similar frauds or bribery incidents;
* investigate whether there has been a failure in supervision and take appropriate disciplinary action where supervisory failures occurred; and
* record and report all discovered cases of fraud/bribery.

## 4.3 Managers

Managers are the first line of defence against fraud/bribery. They should be alert to the possibility that unusual events may be symptoms of fraud/bribery or attempted fraud/bribery and that fraud/bribery may be highlighted as a result of management checks or be brought to attention by a third party. They are responsible for:

* being aware of the potential for fraud;
* being aware of the potential for bribery to take place;
* ensuring that an adequate system of internal control exists within their area of responsibility, appropriate to the risk involved and those controls are properly operated and complied with;
* reviewing and testing control systems to satisfy themselves the systems continue to operate effectively.

# 5. Individual staff

It should be highlighted that all staff have a responsibility to prevent and detect fraud, and as such the following policies and principles apply:

* PRRT staff must have, and be seen to have, the highest standards of honesty, propriety and integrity in the exercise of their duties.
* PRRT will not tolerate fraud, bribery, impropriety or dishonesty and will investigate all instances of suspected fraud, bribery, impropriety, or dishonest conduct by staff or external organisations (contractor or client).
* PRRT staff must not defraud the company, other staff, clients or contractors, in any way.
* PRRT staff must not pay bribes or offer improper inducements to anyone for any purpose, nor should staff accept bribes or improper inducements.
* At all times PRRT staff must ensure they are in compliance with the Gifts and Hospitality policy which can be found in the Finance Manual.
* PRRT will take action – including dismissal and/or criminal prosecution - against any member of staff defrauding (or attempting to defraud) the company and or bribing other staff, clients or contractors, in any way
* PRRT will consider taking action against any previous employees if a fraud/bribery issue arises after they have left PRRT’s employment.
* PRRT will take action - including criminal prosecution - against external organisations or associates defrauding (or attempting to defraud)/bribing the company, other staff, clients or contractors,
* PRRT will co-operate fully with an external investigating body.
* PRRT will always seek to recover funds lost through fraud or bribery.

# 6. What to do if you wish to report a fraud?

PRRT has established arrangements for staff to report any suspicions of fraud without fear of prejudice or harassment. All matters will be dealt with in confidence and in strict accordance with the terms of the Public Interest Disclosure (NI) Order 1998.This statute protects the legitimate personal interests of staff. Vigorous and prompt investigations will be carried out into all cases of actual or suspected fraud discovered or reported. For the procedures to be adopted in all instances of fraud or suspected fraud, please refer to the **Fraud Response Plan in Appendix A**.

# 7. Conclusion

The circumstances of individual frauds will vary. PRRT takes fraud very seriously and will ensure that all cases of actual or suspected fraud, including attempted fraud, are vigorously and promptly investigated and that appropriate remedial action is taken. Managers should be fully aware of their responsibility to protect public funds and as such, should always be alert to the potential for fraud.

Any queries in connection with this policy document should be directed to the Head of Finance and Shared Services.

# Appendix A - Fraud Response Plan

**Introduction**

PRRT has prepared this Fraud Response Plan to act as a procedural guide and provide a checklist of the required actions, which **must** be followed, in the event of a fraud, or attempted fraud, being suspected.

This Fraud Response Plan applies to all monies/personal gains for which the PRRT is accountable.

Adherence to the Fraud Response Plan will enable PRRT to:

* Take timely and effective action to prevent further losses;
* Help to recover losses;
* Establish and secure evidence necessary for possible criminal and disciplinary action;
* Comply with the external reporting requirements set out in Managing Public Money Northern Ireland (MPMNI); and
* Highlight areas of weakness in the operating systems to prevent future losses.

**Preliminary Stage**

In the event of a fraud, attempted fraud or other illegal act being suspected, the officer should immediately report the matter to their line manager/Head of Department. If there is concern that line management may be involved, the matter should be reported to the Head of Finance and Shared Services. If there is any suggestion that the Chief Executive or The Head of Finance and Shared Services are involved in the fraud, the Head of Internal Audit at DOJ should be contacted.

Line management **should not** undertake preliminary enquiries until any suspicion has been reported to and advice taken from the Head of Finance and Shared Services and the HR manager. **It is imperative that enquiries should not prejudice subsequent investigations or corrupt evidence, therefore, IF IN DOUBT, ASK FOR ADVICE.**

A whistleblowing policy is included in the HR manual and this should be consulted by any member of staff who suspects fraud.

The Head of Finance and Shared Services and the HR manager will advise on an initial fact finding exercise. PRRT may wish to contact Internal Audit at DOJ for advice. This discreet preliminary enquiry should be carried out as speedily as possible. Where the suspected fraud involves the use of computers, advice must be sought from the PRRT IT Manager before access or removal of computer equipment is attempted. Consideration should also be given to removing the suspect’s access to computer systems.

The purpose of the initial fact-finding exercise is to determine the factors that gave rise to the suspicion and to clarify whether a genuine mistake has been made or if it is likely that a fraud has been attempted or occurred. This should involve consideration of the source of discovery, the authenticity of the information initially received and line management’s initial assessment of the circumstances involved. It may also involve discreet enquiries with staff or the examination of documents. **It is imperative that such enquiries should not prejudice subsequent investigations or corrupt evidence, therefore, IF IN DOUBT, ASK FOR ADVICE.**

If the preliminary enquiry confirms that a fraud has not been attempted or perpetrated, but indicates that internal controls are deficient, management should review their control systems with a view to ensuring that they are adequate and effective. A robust review of the Department/Department Risk Register should be conducted and where appropriate the Corporate Risk Register should also be reviewed. Internal Audit is available to offer advice and assistance on matters relating to internal control, if required

**Formal Reporting Stage**

If the preliminary enquiry confirms the suspicion that a fraud has been attempted or perpetrated, management must ensure that all original documentation and computer based files are preserved in a safe place for further investigation. Evidence must be carefully preserved; no marks should be made on original documents; and a record should be kept of anyone handling evidence. This is to prevent the loss or corruption of evidence, which may be essential to support subsequent disciplinary action or prosecution. The facts should be reported immediately to the:

* Chief Executive;
* Head of Department concerned;
* Head of Internal Audit;
* Chair of Audit Committee;
* Chair of PRRT Board; and
* Head of Sponsor Branch in DOJ.

To remove any threat of further fraud or loss, management should immediately change/strengthen procedures and if appropriate, suspend any further payments to suppliers pending full investigation. Where the fraud has been perpetrated externally management should consider the need to inform other government departments or bodies.

**Action Required for Internal Fraud**

Where there is the suspicion of staff being involved (internal fraud) the Head of Finance and Shared Services, in consultation with the HR manager and the Head of Internal Audit, will decide on the appropriate course of action including internal reporting and oversight arrangements and the full formal investigation arrangements.

The investigation will be led by Internal Audit and should be conducted by at least two officers, one of whom is trained in investigative techniques. An individual qualified in the use of the Police & Criminal Evidence (PACE) Act will be commissioned as appropriate. Should further expertise be required, e.g. Specialist Fraud Investigators, Forensic Accountants etc., the Head of Finance and Shared Services will contact the DOJ Departmental Establishment Officer (DEO) who will advise us on the engagement of the appropriate assistance.

It is PRRT’s policy to suspend an individual suspected of fraudulent activity at the earliest juncture. Suspension itself does not imply guilt – it is simply another safeguard to prevent the removal or destruction or alteration of evidence.

**Action Required for External Fraud**

Where a fraud is suspected involving an external organisation or individual the Head of Finance and Shared Services should be notified and they in will notify the Chief Executive and the Internal Audit at DOJ. In these cases, it is the responsibility of, Chief Executive in consultation with Head of Finance and Shared Services and the Head of Internal Audit, to determine an appropriate course of action.

If there is sufficient evidence, PRRT should notify the police. Thereafter, the investigation will be guided by police advice.

**Liaison with the Police Service of Northern Ireland**

A Memorandum of Understanding (MOU) between the Northern Ireland Public Sector and the PSNI was formally signed on 30 October 2006 and was updated and revised in September 2010. The MOU sets out a basic framework for the working relationship between the PSNI and the Public Sector in respect of the investigation and prosecution of fraud cases.

Its aim is to ensure consistency in the way fraud cases are investigated across the range of public sector bodies and a more targeted approach to criminal prosecution cases. Details of the arrangement are contained in the DFP, Accountability and Financial Management Division website, under Fraud and Internal Policy Branch.

**Post Event Action**

Appropriate steps will be taken to recover all losses resulting from fraud, if necessary through civil action. PRRT solicitors should be consulted at an early stage on the recovery of assets, for example, action that might be taken to trace and freeze assets; action to prevent the release of assets; obtaining search orders.

Where a fraud, or attempted fraud, has occurred, management must make any necessary changes to systems and procedures to ensure that similar frauds or attempted frauds will not recur. Additionally, if a PRRT employee is suspected of involvement, the Chief Executive in consultation with the Head of Finance and Shared Services will consider the appropriate course of action. This may range from close monitoring/supervision to re-location to precautionary suspension. It should be noted, however, that suspension does not in any way imply guilt.

Internal Audit at DOJ is available to offer advice and assistance on matters relating to internal control, if considered appropriate.

The PRRT Audit Committee should be kept informed of progress during an investigation.

R**eporting Arrangements**

The Head of Internal Audit is responsible for notifications to the Department of Finance and Personnel’s Fraud and Internal Audit Policy Branch (FIAP) and the Comptroller and Auditor General about all discovered fraud, proven or suspected, including attempted fraud, within or against PRRT.

PRRT’s Finance team will submit annual fraud returns to DOJ who in turn will be responsible for compiling the annual return of frauds to DFP (Fraud and Internal Audit Policy). Annex 4.7 of MPMNI defines requirements.

**Investigation of Suspected Fraud**

The following best practice guidance must be applied (as appropriate) during any suspected fraud investigation:

* All aspects of the suspected officer’s work should be investigated, not just the area where the fraud was discovered;
* The investigation will cover the period the officer was responsible for the processes under investigation but consideration should also be given to investigating earlier periods of employment;
* Potential evidence, including paper files, computer files and records of amendments to files relevant to the case, should be retained securely (in compliance with PACE requirements) and not disposed of per normal routine procedures for disposal;
* Control weaknesses discovered in procedures during the investigation should be strengthened immediately to ensure that similar frauds or attempted frauds will not recur;
* The extent, if any, of supervisory failures should be examined.

**Conclusion**

Any queries in connection with this Fraud Response Plan should be made to the Head of Finance and Shared Services.

**Fraud Indicators**

Fraud indicators are clues or hints that a closer look should be made at an individual, area or activity. Examples of issues that could be investigated to ensure fraud is not taking place include:

* Unusual employee behaviour (e.g. a supervisor who opens all incoming mail, refusal to comply with normal rules and practices, failure to take leave, managers by-passing subordinates, subordinates by-passing managers, living beyond means, regular long-hours working, job dissatisfaction/unhappy employee, secretiveness or defensiveness).
* Unrecorded transactions or missing records (e.g. invoices or contracts).
* Disorganised operations in such areas as accounting, purchasing or payroll.
* Crisis management coupled with a pressured business environment.
* Absence of controls and audit trails (e.g. Inadequate or no segregation of duties, lack of rotation of duties).
* Low levels of review or approval.
* Policies not being followed.
* Inadequate monitoring to ensure that controls work as intended (periodic testing and evaluation).
* Lack of interest in, or compliance with, internal controls.
* Documentation that is photocopied or lacking essential information.
* Alterations to documents.
* Missing documents such as expenditure vouchers and official records.
* Excessive variations to budgets or contracts.
* Bank and ledger reconciliations are not maintained or cannot be balanced.
* Excessive movements of cash or transactions between accounts.
* Numerous adjustments or exceptions.
* Duplicate payments.
* Large payments to individuals.
* Unexplained differences between inventory checks and asset or stock records.
* Transactions not consistent with the entity’s business
* Deficient screening for new employees including casual staff, contractors and consultants.
* Employees in close relationships in areas where segregation of duties is a key control.
* Unauthorised changes to systems or work practices.
* Lowest tenders or quotes passed over with minimal explanation recorded.
* Single vendors.
* Unclosed but obsolete contracts.
* Defining needs in ways that can be met only by specific contractors.
* Splitting up requirements to get under small purchase requirements or to avoid prescribed controls.
* Suppliers/contractors who insist on dealing with one particular member of staff.
* Vague specifications.
* Disqualification of any qualified bidder.
* Chronic understaffing in key control areas.
* Excessive hours worked by key staff.
* Consistent failures to correct major weaknesses in internal control.
* Management frequently override internal control.
* Lack of common sense controls such as changing passwords frequently, requiring two signatures on cheques or restricting access to sensitive areas.