



**AGRI-FOOD  
& BIOSCIENCES  
INSTITUTE**

Counter-Fraud Policy &  
Fraud Response Plan  
May 2024, version 9

**afbi**

# Counter-Fraud Policy & Fraud Response Plan

---

The Policy outlines the responsibility of all staff to prevent fraud. It also lays out AFBI's procedures which must be followed if fraud is suspected or detected.

---

<b>Reference<sup>1</sup>:</b>	AFBI POL 01/12
<b>Date:</b>	10 MAY 2021 (EMT Approval) 03 MAR 2016 (Board Approval)
<b>Version:</b>	9.0 (May 24)
<b>Author:</b>	Head of Governance & Performance

---

<sup>1</sup> Reference number is provided by Governance & Performance Branch

## Version Control

Version	Date of issue	Reason for issue
Version 1.0	February 2012	First issue
Version 3.0	June 2014	Removal of Gifts & Hospitality
Version 4.2	March 2015	Removal of whistle-blowing policy Incorporates the requirements of the Bribery Act 2010
Version 5.0	February 2016	Replacement of CIS with DFP FIS Updated proforma (Appendix 6) Addition of Head of Governance & Performance as a designated senior manager Inclusion of sanction and redress section in response plan
Version 6.0	March 2017	Revised Flowcharts to ensure clarity Updated references to DAERA
Version 7.0	March 2020	Updated to designate role of Head of Governance & Performance as SRO for managing fraud risk at an organisational level. Updated to highlight that regular Fraud awareness training will be provided to staff and this will be included as part of the staff induction process.
Version 8.0	April 2021	Formatted to reflect AFBI's new policy template Referenced legislation checked to ensure they are current Reference to NICS Fraud Forum removed and replaced with Group Fraud Investigation Service (GFIS)
Version 9.0	May 2024	Routine Review with no significant changes

## Contents

1	INTRODUCTION .....	1
2	WHAT IS FRAUD? .....	2
2.1	Types of Fraud .....	3
2.2	The Bribery Act 2010 .....	4
2.2.1	Applicability: .....	4
3	ROLES AND RESPONSIBILITIES .....	5
3.1	AFBI's Responsibilities.....	5
3.2	Line Managers' Responsibilities.....	5
3.3	Staff Responsibilities .....	6
3.4	Internal Audit.....	7
3.5	Counter Fraud Forum.....	8
4	FRAUD RISK ASSESSMENTS.....	9
5	FRAUD INVESTIGATION .....	10
5.1	Investigation Principles .....	10
5.2	Sanction/Action.....	11
5.3	Malicious Allegations .....	11
6	Conclusion .....	11
7	FRAUD RESPONSE PLAN .....	13
7.1	Overarching theme of the Fraud Response Plan:.....	13
7.2	Preliminary Stage (see flowchart in <b>Appendix G</b> refers) .....	13
7.3	Formal Reporting Stage (Internal Fraud).....	14
7.4	Liaison with the Police Service of Northern Ireland .....	15
7.5	Sanction and Redress .....	16
7.6	Post Event Action.....	16
7.7	Communication.....	17
7.8	Conclusion.....	17
8	Monitoring and Review .....	17
	APPENDIX A – Indicators of Fraud.....	18
	APPENDIX B – Common Methods and Types of Fraud .....	20
	APPENDIX C – Examples of Good Management Practices Which May Assist in Combating Fraud .....	21
	APPENDIX D – Best Practice for Reporting Suspicions of Fraud and Irregularity .....	23
	APPENDIX E – Guidance on Performing an Assessment of Fraud Risks and Completion of Template.....	24
	APPENDIX F – AFBI Fraud Report Pro-Forma.....	28
	APPENDIX G – Reporting Fraud/Suspected Fraud .....	31
	APPENDIX H – Contact Details .....	32
	APPENDIX I – Memorandum of Understanding .....	33

# INTRODUCTION

Like any financial organisation AFBI is susceptible to deliberate and opportunistic fraud and abuse. The circumstances in which it can exist are diverse.

The opportunity to commit fraud is therefore ever-present, and hence must be a concern to all members of staff. It is everyone's responsibility to prevent fraud and follow AFBI's procedures where a fraud is suspected or detected.

This policy outlines the commitment AFBI places on the prevention and detection of fraud and irregularity and provides guidance to colleagues on these important issues.

Guidance on staff conduct regarding offers and the acceptance of gifts, rewards and hospitality, and whistleblowing are contained in separate guidance issued by AFBI and is available on the AFBI website.

AFBI operates a **"zero tolerance"** policy with regard to fraud. All potential or actual frauds will be thoroughly investigated with the aim of establishing the facts. If fraud occurs AFBI will take the appropriate legal and/or disciplinary action in all cases where that would be justified; and will make any necessary changes to systems and procedures to ensure that similar frauds will not happen again.

AFBI's Annual Report will disclose certain categories of external and internal fraud and irregularity attempted or perpetrated against AFBI and, where appropriate, the outcome of these investigations. AFBI publicises all fraud prosecutions as a deterrent to those intending to commit fraud.

Potential outcomes when fraud is proved:

- discipline, which may include dismissal, of any member(s) of staff who have engaged in or attempted fraud;
- criminal prosecution, as directed by the Public Prosecution Service, on the recommendation of the Department of Finance (DOF) Group Fraud Investigation Service (GFIS), of all individuals responsible for fraud.

## WHAT IS FRAUD?

Fraud is the obtaining of financial advantage or causing of loss by implicit or explicit deception: it is the mechanism through which the fraudster gains unlawful advantage or causes unlawful loss.

Fraud is a **crime** in which common elements include:

1. Dishonesty
2. An acquisition or obtaining
3. A falsehood or deception

The term 'fraud' is used to describe such acts as deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts and collusion.

Computer fraud is where information technology (IT) equipment has been used to manipulate computer programs or data dishonestly (for example by altering or substituting records, destroying or suppressing records, duplicating or creating spurious records), or where the existence of an IT system was a material factor in the perpetration of fraud (i.e. where the fraud was unlikely to have occurred if there had been no IT system). Theft or fraudulent use of computer facilities, computer programs and the internet is included in this definition. The suspicion that any of these acts have taken place should be regarded as potentially fraudulent. In this regard, staff should note that e-mails relating to official AFBI business sent by staff from private e-mail accounts to third parties (i.e. persons who are not members of AFBI staff) must always be copied to the staff member's official AFBI e-mail address, so that there is an official record of the communication.

## Types of Fraud

There are a number of criminal offences that relate to what we might commonly term as “fraud” and are covered by the Theft Act (Northern Ireland) 1969 and the Theft (Northern Ireland) Order 1978. However the Fraud Act 2006 created a new general offence of fraud with three possible ways of committing it.

- i. **Fraud by false representation**, i.e. if an individual dishonestly makes a false representation and intends by making the representation to make a gain for himself or another, or to cause loss to another or expose another to risk of loss;
- ii. **Fraud by failing to disclose information**, i.e. if an individual dishonestly fails to disclose to another person information which he is under a legal duty to disclose and intends, by means of abuse of that position, to make a gain for himself or another, or to cause loss to another or expose another to risk of loss; and
- iii. **Fraud by abuse of position**, i.e. if an individual occupies a position in which he is expected to safeguard, or not to act against, the financial interests of another person, and he dishonestly abuses that position, and intends, by means of the abuse of that position, to make a gain for himself or another, or to cause loss to another or to expose another to a risk of loss.

The Fraud Act 2006 supplements the Theft Act (Northern Ireland) 1969 and the Theft (Northern Ireland) Order 1978, which have traditionally been used to cover acts of fraud.



## The Bribery Act 2010

DAO (DOF) 09/11 Bribery Act 2010 clarifies how the Bribery Act 2010 applies to public servants in Northern Ireland.

The Bribery Act 2010 is concerned with bribery. Very generally, this is defined as giving or accepting a financial or other advantage to encourage the performance of functions or activities improperly or to reward a person for having already done so. This could therefore cover seeking to influence a decision-maker by giving an extra benefit to that decision maker rather than by what can legitimately be offered as part of a tender process. The Bribery Act 2010 is not concerned with fraud, theft, books and record offences, Companies Act offences, money laundering offences or competition law.

1. The UK Bribery Act 2010 came into effect on 1 July 2011 and introduced four new statutory offences. The first three relate to individuals and the other is corporate. Bribing another person (active bribery) (Section 1 of the Act); and
2. Being bribed (passive bribery) (Section 2 of the Act).
3. Bribery of a foreign public official (Section 6) and
4. Failure of commercial organisations to prevent bribery by persons associated with them (Section 7). AFBI qualifies as a commercial organisation for the purposes of this section.

### Applicability:

The Bribery Act 2010 applies equally to individuals in public service as it applies to all other individuals. In practice this means that any individual or employee who bribes another person or is bribed is liable to prosecution under the Bribery Act 2010.

The Standards of Conduct of all staff are set out within the NICS HR Handbook Section 6.01 (Standards of Conduct), which indicates that all staff should conduct themselves with honesty and impartiality at all times. Hence it is not acceptable to receive any benefit that may be perceived as having the potential to compromise personal judgement on work related issues.

# ROLES AND RESPONSIBILITIES

## AFBI's Responsibilities

AFBI's responsibilities are set out in Annex 4.7 of Managing Public Money Northern Ireland (MPMNI), and the reporting of fraud to the Department of Agriculture, Environment and Rural Affairs (DAERA) is set out in paragraphs 80-81 of the AFBI Management Statement and Financial Memorandum. Also, DAO (DOF) 06/11 contains a booklet entitled '*Managing the Risk of Fraud – A Guide for Managers*', with which all managers and staff should be familiar.

To enhance understanding and compliance, AFBI staff will be provided with appropriate education and training. This will include regular mandatory fraud awareness training and inclusion of this training for the induction of all new staff. In addition, AFBI shall report immediately to AFBI Sponsor Branch (ASB) all frauds (proven or suspected), including attempted fraud and the quarterly fraud returns, commissioned by DOF via ASB.

AFBI's Accounting Officer is responsible for establishing and maintaining a sound system of internal control that supports the achievement of AFBI's policies, aims and objectives. The system of internal control is designed to respond to and manage the whole range of risks that AFBI faces.

The system of internal control is based on an on-going process designed to identify the principal risks, to evaluate the nature and extent of those risks and to manage them effectively. Managing fraud risk will be seen in the context of the management of this wider range of risks.

Although the Accounting Officer bears overall responsibility and is liable to be called to account for specific failures, these responsibilities fall directly on line management and may involve individual AFBI staff.

AFBI's Head of Governance and Performance is the designated Senior Responsible Owner for Managing the risk of Fraud at an organisational level.

## Line Managers' Responsibilities

Line managers are personally responsible for ensuring that an adequate system of internal control exists within their areas of responsibility and that controls operate effectively. The responsibility for the prevention and detection of fraud rests primarily with managers.

All managers need to assess the types of risk involved in the business area for which they are responsible, to review and test regularly the control systems for

which they are responsible, to ensure that controls are being complied with, and to satisfy themselves that their systems continue to operate effectively. A formal detailed assessment of the fraud risks facing each business area must be completed annually.

Managers are also responsible for ensuring that when designing and implementing new policies, programmes and systems that good controls are built in to prevent and detect fraud. Advice can be provided in relation to fraud risk and control matters by the Head of Governance and Performance (HoGP).

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

## Staff Responsibilities

Every member of staff has a duty to ensure that public funds are safeguarded whether they are involved with cash, payments systems, receipts, stocks, contractors and suppliers and therefore, everyone is responsible for:

- (a) Acting with propriety in the use of official resources and the handling and use of public funds in all instances. This includes cash and/or payment systems, receipts and dealing with suppliers;
- (b) Conducting themselves in accordance with the seven principles of public life detailed in the first report of the Nolan Committee 'Standards in Public Life', i.e. selflessness, integrity, objectivity, accountability, openness, honesty and leadership; and
- (c) Being vigilant to the possibility that unusual events or transactions could be indicators of fraud and alerting their line manager where they believe the opportunity for fraud exists. [Appendix A](#) provides examples of Fraud Indicators. In addition, Common Methods and Types of Fraud are included in [Appendix B](#), with examples of Good Management Practices which may assist in combating fraud detailed in [Appendix C](#).

In addition, it is the **responsibility** of every member of staff to report details immediately if they suspect that a fraud has been attempted or committed, or see any suspicious acts or events. (See [Appendix D - Best Practice for Reporting Suspicions of Fraud and Irregularity](#))

A description of the constitutional position of Civil servants and the values they are expected to uphold is given in the NICS code of Ethics. (See NICS Staff Handbook – HR Connect Portal). This applies equally to AFBI staff.

The Public Interest Disclosure (NI) Order 1998 – see AEC 83/08 (Guidance on Public Interest Disclosure ('whistleblowing')) – protects the rights of staff who report

wrongdoing. Guidance on Whistleblowing can be found in AFBI's Whistleblowing Policy. <http://afbi.intranet.nigov.net/publications/whistleblowing-policy-procedures-and-guidance>.

Section 5 of the Criminal Law Act (Northern Ireland) 1967 (Withholding Information) also places the onus on individuals to report/pass evidence of suspected fraud to the Police. The involvement of the Police Service of Northern Ireland (PSNI) is dealt with in the Fraud Response Plan.

Staff must also assist any investigations by making available all relevant information, by co-operating in interviews and if appropriate provide a witness statement.

As stewards of public funds, public servants must have, and be seen to have, high standards of personal integrity. Staff should not accept gifts, hospitality or benefits of any kind from a third party, which might be seen to compromise their integrity. Separate guidance has been issued on AFBI's Gifts and Hospitality Guidelines.

It is also essential that staff understand and adhere to systems and procedures including those of a personnel/management nature such as submission of expenses claims and records of absence, flexi and annual leave.

## Internal Audit

Internal Audit is responsible for the provision of an independent and objective opinion to the Accounting Officer on risk management, control and governance. The adequacy of arrangements for managing the risk of fraud and ensuring AFBI promotes an anti-fraud culture is a fundamental element in arriving at an overall opinion.

Internal Audit has no responsibility for the prevention or detection of fraud. However, Internal Audit provides assistance by examining and evaluating the adequacy and effectiveness of management's action to fulfil their obligation. Internal Audit's responsibilities in relation to fraud are to:-

- (a) carry out audit assignments using due professional care and in such a way as to be alert to the possibility of fraud and misconduct;
- (b) review procedures to safeguard assets so as to ensure that cost effective measures are in place to prevent, detect or defer fraud;
- (c) ensure that the prevention, detection and deterrence of fraud are also taken into account when new systems are designed or changes made to existing systems; and

- (d) provide assistance, where required by management, in the investigation of fraud, but with a clear understanding that in so doing they are not fulfilling their primary internal audit role.

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

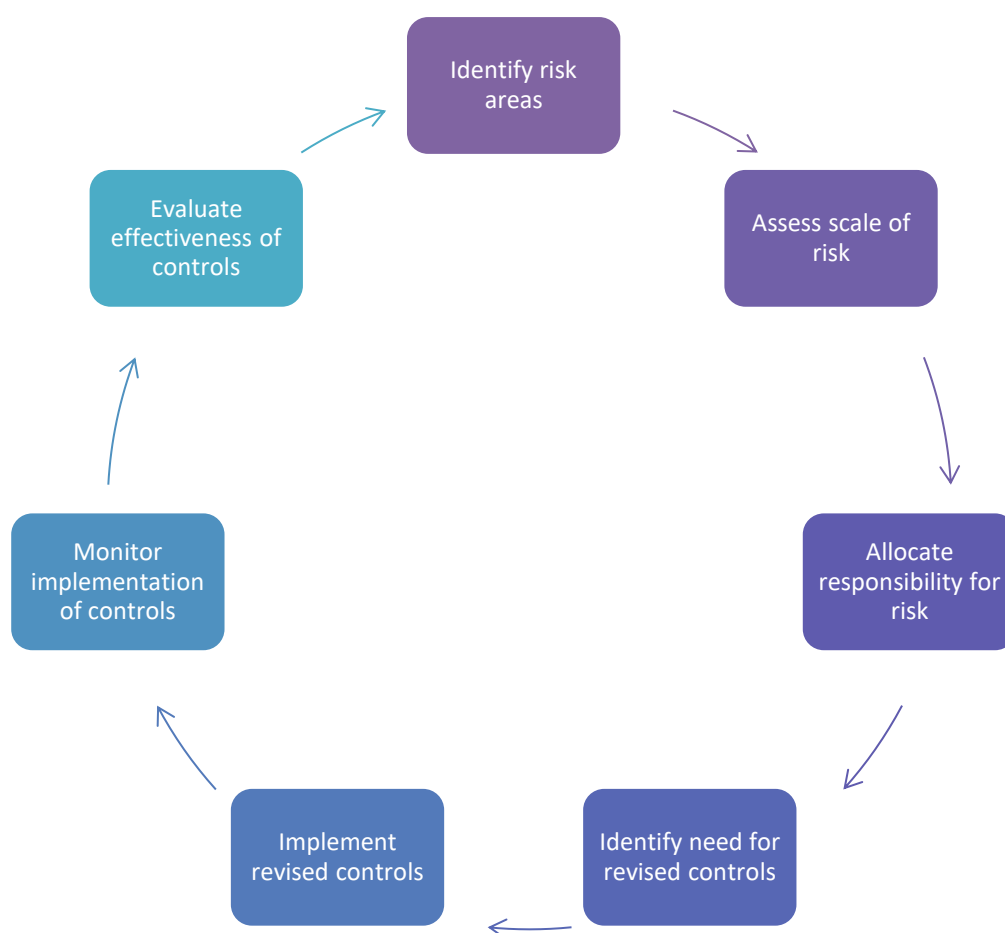
## Counter Fraud Forum

The DAERA Principal Accounting Officer has established the Counter Fraud Forum as a subcommittee of the DAERA Audit & Risk Assurance Committee (ARAC), and one of the responsibilities of this forum is to invite the DAERA NDPBs to attend. AFBI's attendance helps in ensuring that its Counter Fraud Strategy remains relevant, effective and reflects current best practice.

The Forum is advisory in nature and its primary role is to oversee, promote and provide input to all activities associated with countering fraud. The Forum meets on a quarterly basis and more often if required.

## FRAUD RISK ASSESSMENTS

A major element of good corporate governance is a sound assessment of the organisation's business risks. The key to managing the risk of fraud is the same in principle as managing any other business risk and should be approached systematically at both the organisational and the operational level. The assessment of risk should be part of a continuous cycle rather than a one-off event: as systems and the environment change, so do the risks to which AFBI will be exposed. The figure below sets out the key stages of a risk management cycle to help deal with fraud. Please see [Appendix E](#) - Guidance on Performing an Assessment of Fraud Risks. These are to be completed every 2 years which is in line with NIAO guidance.



## FRAUD INVESTIGATION

AFBI's Head of Governance & Performance (HoGP) in consultation with the CEO will determine what action needs to be taken in circumstances where the suspected **internal** fraud involves large amounts of money or if the case is of a serious or complicated nature or the additional powers of the police are required to complete the investigation.

The HoGP will ensure the following best practice guidance is applied during an **internal** investigation.

- **All aspects** of the suspected officer's work is investigated, not just the area where the fraud was discovered.
- The investigation will obviously 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 computer files and record of amendments relevant to the case **should be retained securely** (in compliance with PAC requirements) and not disposed of per the normal routine procedures for disposal.
- Control weaknesses discovered in procedures during the investigation should be **strengthened immediately**.
- The extent, if any, of **supervisory failures** should be examined.

AFBI is included in a Service Level Agreement agreed between DAERA and the DOF Group Fraud Investigation Service (GFIS). Under this agreement AFBI may decide to use GFIS to carry out an investigation where fraud, irregularity or breaches of regulatory legislation is suspected. A GFIS referral proforma will be completed by the HoGP if this action is agreed.

### Investigation Principles

Line managers should be alert to the possibility that unusual events or transactions could be symptoms of fraud or attempted fraud. Fraud may also be highlighted as a result of specific management checks or be brought to management's attention by a third party.

It is AFBI's policy that there will be consistent handling of all suspected fraud cases without regard to position held or length of service of the individual(s) involved.

Investigators should have free access to all staff, records and premises in order to carry out investigations.

Irrespective of the source of suspicion, it is for the relevant Head of Division to undertake an initial investigation to ascertain the facts. (They may seek assistance from the HoGP). This investigation should be carried out as speedily as possible after suspicion has been aroused: **prompt action is essential.**

**The purpose of the initial investigation is to confirm or repudiate the suspicions that have arisen so that, if necessary, further investigation may be instigated. However, as detailed in the Fraud Response Plan, It is imperative that such enquiries should not prejudice subsequent investigations or corrupt evidence, therefore, ASK FOR ADVICE (from the HoGP).**

Once suspicion has been aroused that a fraud may have been perpetrated, management should follow the guidance provided in the attached Fraud Response Plan.

## Sanction/Action

After a full investigation AFBI will take legal and/or disciplinary action in all cases where it is considered appropriate. Where supervisory negligence is found to be a contributory factor, disciplinary action may also be initiated against those managers/supervisors responsible. Any member of staff found guilty of a criminal act will be considered to have committed a serious disciplinary offence and is likely to be dismissed from AFBI on the grounds of gross misconduct.

AFBI HR may suspend or redeploy any officer involved, pending the outcome of an investigation. Suspension or redeployment itself does not imply guilt.

In all cases of fraud, whether perpetrated or attempted by a member of staff or by external organisations or persons, AFBI will consider referring the case to the Police Service of Northern Ireland at the earliest possible juncture.

Losses resulting from fraud should be recovered, subject to the policy on write-off, if necessary through civil action.

## Malicious Allegations

If an allegation is made frivolously, in bad faith, maliciously or for personal gain, disciplinary action may be taken against the person making the allegation.

## Conclusion

It is appreciated that the circumstances of individual frauds will vary but it is important that all are vigorously and promptly investigated and that appropriate remedial action is taken. Management should be conscious of their responsibility to protect public funds and as such, should always be alert to the potential for fraud.

The HoGP is available to offer advice and assistance on risk management/internal control issues or Internal Audit is available if considered appropriate.

## FRAUD RESPONSE PLAN

The purpose of the Fraud Response Plan is to provide guidance and act as a checklist to all AFBI managers which they **must** follow in the event that they suspect fraud or irregular activity to be taking place.

Adherence to the Fraud Response Plan will enable AFBI 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;
- Notify DOF and NIAO of such instances as per Managing Public Money(Northern Ireland) Instruction; and
- Highlight areas of weakness in the operating systems to prevent future losses.

The Plan provides staff with information regarding the reporting lines, authority levels and responsibilities for action in the case of a suspected fraud.

Overarching theme of the Fraud Response Plan:

***‘IF IN DOUBT, ASK THE HoGP OR  
INTERNAL AUDIT FOR ADVICE’.***

### Preliminary Stage (see flowchart in [Appendix G](#) refers)

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 Branch. If there is concern that line management may be involved, the matter should be reported to the next appropriate level. Where confidentiality is sought, staff may report their suspicions directly to the HoGP or CEO.

It is for Head of Division to undertake an initial fact-finding exercise. **It is imperative that such enquiries should not prejudice subsequent investigations or corrupt evidence, therefore, SEEK ADVICE on how to proceed.** The HoGP can be contacted for advice on **how to correctly proceed** at the preliminary enquiry stage and on what further enquiries are necessary or the

Head of Internal Audit can also provide advice. [Appendix H](#) provides contact details.

This discreet preliminary enquiry should be carried out as speedily as possible and certainly within 24 hours of the suspicion being raised. The purpose of the initial fact-finding exercise is to determine the factors that gave rise to 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 may involve discreet enquiries with staff or the examination of documents.

If the preliminary enquiry confirms that a fraud has not been attempted nor perpetrated, but, internal controls are deficient, management should review their control systems with a view to ensuring they are adequate and effective, and where relevant the Risk and Control Framework should be updated and, where appropriate, the Branch and Corporate Risk Register(s). Internal Audit is available to offer advice and assistance on matters relating to internal control, if required.

### Formal Reporting Stage (Internal Fraud)

If the preliminary enquiry confirms the suspicion that a fraud has been attempted or perpetrated, management must ensure that all original documentation is preserved in a safe place for further investigation. This is to prevent the loss of evidence, which may be essential to support subsequent disciplinary action or prosecution.

The suspected fraud must be reported immediately to the HoGP.

The AFBI Fraud Report Pro-Forma ([Appendix F](#)) should be completed as soon as possible by the Division concerned and forwarded to the HoGP who will arrange for the suspected fraud to be reported immediately to CEO the CEO, AFBI Sponsor Branch , the Comptroller and Auditor General (C&AG) and the Head of Internal Audit. Information on reported internal frauds will be provided to AFBI's Audit & Risk Assurance Committee

The HoGP will assess the preliminary enquiry findings to determine the scope of the investigation. In circumstances where the suspected **internal** fraud involves large amounts of money or if the case is of a serious or complicated nature the HoGP will defer to the CEO who will decide if the police should be approached to complete the investigation.

To remove any threat of further fraud or loss, management should immediately change/strengthen procedures and if appropriate, suspend any further payments pending full investigation.

The HoGP will decide in consultation with the CEO on the appropriate course of action including the full formal investigation arrangements and the scope of the investigation. If further expertise is required, e.g. Solicitors, Forensic Accountants/Engineers, the HoGP will engage the appropriate assistance taking due care not to breach any procurement guidelines.

The HoGP should agree the Terms of Reference for the investigation with the expert and draw up an oversight/checkpoint plan for the various stages of the investigation.

The HoGP should ensure the following best practice guidance is applied during an **internal** investigation. **All aspects** of the suspected officer's work should be investigated, not just the area where the fraud was discovered.

- The investigation will obviously 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 computer files and record of amendments relevant to the case **should be retained securely** (in compliance with the Police and Criminal Evidence (Northern Ireland) Order 1989 Codes of Practice requirements) and not disposed of per the normal routine procedures for disposal.
- Control weaknesses discovered in procedures during the investigation should be **strengthened immediately**.
- The extent, if any, of **supervisory failures** should be examined.

## Liaison with the Police Service of Northern Ireland

A Memorandum of Understanding (MoU) has been agreed with the Police Service of Northern Ireland (PSNI) Fraud Unit for the Public Sector. The MoU provides a basic framework for the working relationships between the NI Public Sector and the PSNI in respect of the investigation and prosecution of suspected fraud cases and is attached at [Appendix I](#) of this document.

PSNI is available to give advice and/or guidance in cases where fraud is suspected (contact details are available in the Annex B of the MoU; [Appendix I](#) refers). Where actual or attempted fraud is confirmed and is of a large or complex nature, the Fraud Squad is capable of carrying out investigations. Smaller cases may be referred to the local police.

## Sanction and Redress

Appropriate steps will be taken to recover all losses resulting from fraud, if necessary through civil action. There are three main actions that AFBI may pursue as part of its fraud investigation which will be completed via the DoF GFIS:

- I Conduct the investigation to a criminal standard to maximise the opportunities for a criminal prosecution. This course of action may include the preparation and submission to the PSNI of an evidential pack. Alternatively, where in-house expertise is available, the investigation can be taken forward with a view to presenting a file to the Public Prosecution Service for direction;
- II Seek redress of any outstanding financial loss through the Civil Courts, if appropriate; and
- III Pursue the internal disciplinary process which may, if there is clear evidence of supervisory failures, include other officials.

Each option needs careful consideration in order to decide on the most appropriate course of action to be taken in each case. It is important that any civil/disciplinary action does not impair a criminal investigation and vice versa.

## Post Event Action

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 an AFBI employee is suspected of involvement, the CEO will consider the appropriate course of action. This may range from close monitoring/supervision to precautionary suspension, however, it should be noted that suspension does not in any way imply guilt.

## Communication

The following communications should be observed in all cases:

- AFBI Audit and Risk Assurance Committee should be kept informed of developments during the investigation;
- A lessons-learned document should be circulated throughout AFBI, if appropriate;
- This AFBI Fraud Response Plan should be reviewed to determine whether it needs to be updated and if so, changes should be circulated throughout the organisation;
- Consideration should be given to informing other public sector organisations, e.g. other Government Departments, NIAO, grant paying organizations; and
- At the appropriate time, inform the DOF GFIS of outcomes and lessons learned.

## Conclusion

Any queries in connection with this response plan should be made to the Head of Governance & Performance.

Advice and assistance on risk management/internal control issues can be sought from the Head of Governance & Performance or Head of Internal Audit.

Current contact details for officers referred to above are provided in [Appendix H](#)

## Monitoring and Review

This Policy and Response Plan will be subject to review on a tri-annual basis.

## APPENDIX A – Indicators of Fraud

- Missing expenditure vouchers and unavailable official records
- Crisis management coupled with a pressured business climate
- Profitability declining
- Excessive variations to budgets or contracts
- Refusals to produce files, minutes or other records
- Related party transactions
- Increased employee absences
- Borrowing from fellow employees
- An easily led personality
- Covering up inefficiencies
- Lack of Board oversight
- No supervision
- Staff turnover is excessive
- Figures, trends or results which do not accord with expectations
- Bank reconciliations are not maintained or can't be balanced
- Excessive movement of cash funds
- Multiple cash collection points
- Remote locations
- Offices with excessively flamboyant characteristics
- Employees suffering financial hardships
- Placing undated/post-dated personal cheques in petty cash
- Employees apparently living beyond their means
- Heavy gambling debts
- Signs of drinking or drug abuse problems
- Conflicts of interest
- Lowest tenders or quotes passed over with scant explanations recorded
- Employees with an apparently excessive work situation for their position
- Managers bypassing subordinates
- Subordinates bypassing managers
- Excessive generosity
- Large sums of unclaimed money
- Large sums held in petty cash
- Lack of clear financial delegations
- Secretiveness
- Apparent personal problems

- Unauthorised changes to systems or work practices

- Marked character changes

### **Indicators of Fraud (Continued)**

- |  |   |
|--|---|
| <ul style="list-style-type: none"> <li>• Employees with outside business interests or other jobs</li> <li>• Large outstanding bad or doubtful debts</li> <li>• Poor morale</li> <li>• Excessive control of all records by one officer</li> <li>• Poor security checking processes over staff being hired</li> <li>• Unusual working hours on a regular basis</li> <li>• Refusal to comply with normal rules and practices</li> <li>• Personal creditors appearing at the workplace</li> <li>• Non taking of leave</li> <li>• Excessive overtime</li> <li>• Large backlogs in high risk areas</li> <li>• Lost assets</li> </ul> | <ul style="list-style-type: none"> <li>• Excessive ambition</li> <li>• Apparent lack of ambition</li> <li>• Unwarranted organisation structure</li> <li>• Absence of controls and audit trails.</li> <li>• Socialising with clients – meals, drinks, holidays</li> <li>• Seeking work for clients</li> <li>• Favourable treatment of clients – e.g. allocation of work</li> <li>• Altering contract specifications</li> <li>• Contract not completed to specification</li> <li>• Contractor paid for work not done.</li> <li>• Grants not used for specified purpose – e.g. Leasing capital equipment instead of purchasing them</li> </ul> |
|--|---|

### **Corporate Fraud**

- Lack of thorough investigations of alleged wrongdoing
- Pecuniary gain to organisation – but no personal gain

## APPENDIX B – Common Methods and Types of Fraud

<ul style="list-style-type: none"> <li>• Payment for work not performed</li> <li>• Forged endorsements</li> <li>• Altering amounts and details on documents</li> <li>• Collusive bidding</li> <li>• Overcharging</li> <li>• Writing off recoverable assets or debts</li> <li>• Unauthorised transactions</li> <li>• Selling information</li> <li>• Altering stock records</li> <li>• Altering sales records</li> <li>• Cheques made out to false persons</li> <li>• False persons on payroll</li> <li>• Theft of official purchasing authorities such as order books</li> <li>• Unrecorded transactions</li> <li>• Transactions (expenditure/receipts/deposits) recorded for incorrect sums</li> <li>• Cash stolen</li> <li>• Supplies not recorded at all</li> </ul>	<ul style="list-style-type: none"> <li>• False official identification used</li> <li>• Damaging/destroying documentation</li> <li>• Using copies of records and receipts</li> <li>• Using imaging and desktop publishing technology to produce apparent original invoices</li> <li>• Charging incorrect amounts with amounts stolen</li> <li>• Transferring amounts between accounts frequently</li> <li>• Delayed terminations from payroll</li> <li>• Bribes</li> <li>• Over claiming expenses</li> <li>• Skimming odd pence and rounding</li> <li>• Running a private business with official assets</li> <li>• Using facsimile signatures</li> <li>• False compensation and insurance claims</li> <li>• Stealing of discounts</li> <li>• Selling waste and scrap.</li> </ul>
---	---

## APPENDIX C – Examples of Good Management Practices Which May Assist in Combating Fraud

- All income is promptly entered in the accounting records with the immediate endorsement of all cheques
- Regulations governing contracts and the supply of goods and services are properly enforced
- Accounting records provide a reliable basis for the preparation of financial statements
- Controls operate which ensure that errors and irregularities become apparent during the processing of accounting information
- A strong internal audit presence
- Management encourages sound working practices
- All assets are properly recorded and provision is made known or expected losses
- Accounting instructions and financial regulations are available to all staff and are kept up to date
- Effective segregation of duties exists, particularly in financial accounting and cash/securities handling areas
- Close relatives do not work together, particularly in financial, accounting and cash/securities handling areas
- Creation of an agency climate to promote ethical behaviour
- Act immediately on internal/external auditor's report to rectify control weaknesses
- Review, where possible, the financial risks of employees
- Issue accounts payable promptly and follow-up any non-payments
- Set standards of conduct for suppliers and contractors
- Maintain effective security of physical assets; accountable documents (such as cheque books, order books); information, payment and purchasing systems
- Review large and unusual payments
- Perpetrators should be suspended from duties pending investigation

- Proven perpetrators should be dismissed without a reference and prosecuted
- Query mutilation of cheque stubs or cancelled cheques
- Store cheque stubs in numerical order
- Undertake test checks and institute confirmation procedures
- Develop well defined procedures for reporting fraud, investigating fraud and dealing with perpetrators
- Maintain good physical security of all premises
- Randomly change security locks and rotate shifts at times (if feasible and economical)
- Conduct regular staff appraisals
- Review work practices open to collusion or manipulation
- Develop and routinely review and reset data processing controls
- Regularly review accounting and administrative controls
- Set achievable targets and budgets, and stringently review results
- Ensure staff take regular leave
- Rotate staff
- Ensure all expenditure is authorised
- Conduct periodic analytical reviews to highlight variations to norms
- Take swift and decisive action on all fraud situations
- Ensure staff are fully aware of their rights and obligations in all matters concerned with fraud

AFBI participates in the bi-annual National Fraud Initiative (NFI) and submits data downloads for advanced data matching techniques mainly on trade creditors and payroll. It also follows up, investigates and reports on any mismatches identified as part of the NFI to both EMT and the AFBI Board.

## APPENDIX D – Best Practice for Reporting Suspicions of Fraud and Irregularity

If staff become aware of a suspected fraud or irregularity, write down the concerns immediately. Make a note of all relevant details, such as what was said in phone or other conversations, the date, the time and the names of anyone involved. It may necessary to handover any notes and/or evidence you have gathered to the appropriate investigator.

Staff must **not** do any of the following:

- Contact the suspected perpetrator in an effort to determine the facts.
- Discuss the case facts, suspicions, or allegations with anyone outside AFBI.
- Discuss the case with anyone within AFBI other than the people detailed in the policy and response plan.
- Attempt to personally conduct investigations or interviews or question anyone.

### **Action by Managers**

If Line Management has reason to suspect fraud or corruption in the work area, they should do the following:

Listen to the concerns of your staff and treat every report received seriously and sensitively.

Make sure that all staff concerns are given a fair hearing. Line Management should also reassure staff that they will not suffer because they have told you of the suspicions.

Get as much information as possible from the member of staff, including any notes and any evidence they have that may support the allegation. Do not interfere with any evidence and make sure it is kept in safe place.

Do not try to carry out an investigation yourself; this may damage any criminal enquiry. Seek advice from Head of Internal Audit before taking any action.

Report the matter immediately to Line Management.

## APPENDIX E – Guidance on Performing an Assessment of Fraud Risks and Completion of Template

**1. Identify the key fraud risks facing your business and detail these in Column 1.**

Examples might be:

- Fraudulent subsidy/grant claims;
- Payment made on false documentation;
- Deliberate infection of disease;
- Illegal importation/exportation of animals;
- Theft of assets;
- Misappropriation of cash;
- False accounting;
- Contract fraud;
- Procurement fraud;
- Collusion;
- Computer fraud;
- Fraudulent encashment of payable instruments;
- Travel and subsistence fraud;
- False claims for hours worked; etc.

**2. Assess the impact of the identified fraud risk should it occur – High, Medium or Low (Column 2). What damage could be done in relation to achievement of objectives, financial loss, reputation etc?**

**3. Assess the likelihood of the identified fraud risk occurring – High, Medium or Low (Column 3). High would be probable/likely, low would be improbable/unlikely.**

**4.** Identify the key controls already in place to address each identified risk (Column 4);

Examples might be:

- Segregation of duties;
- Payment authorisation levels;
- Payment/lodgement reconciliations;
- Management checks and reviews;
- Tendering process;
- Transparent approval process;
- Inter-system checks e.g. G&S against APHIS;
- Physical controls such as safes, key safes etc.;
- Logical access controls;
- Physical access controls;
- Asset register and inventory checks;
- Audit logs;
- Project monitoring;
- Performance monitoring;
- Independent/unannounced inspections;
- Post-payment checks;
- Training;
- Manuals;
- Staff rotation;
- Irregularity recording, investigation and reporting process etc.

**5.** Determine if any risk still exists after the application of the identified controls (Column 5). For example, the original risk detailed in column 1 will probably still be a risk post-control

although the effective application of the controls detailed in column 4 will reduce the likelihood of occurrence.

6. Detail in Column 6 what further action you are going to take to address the residual risk. It may be that control over the risk lies elsewhere and as a consequence you will have to accept the risk. If this is the case, justify why you are accepting the risk. If you are planning further action to treat the risk, state what this is, who will be responsible for the action and when it is to be implemented.
7. Column 7 will be used by you for internal reviews of the risk management framework.
8. Issue completed framework to Counter Fraud Forum through the Group Head of Fraud Investigation Service annually. Review internally on a regular basis – at least every 6 months.

Fraud Risk Assessment Template

FRAUD RISK	IMPACT (H, L, M)	LIKELIHOOD (H, L, M)	KEY CONTROLS	RESIDUAL RISKS	PLANNED ACTION	ACTION TAKEN

## APPENDIX F – AFBI Fraud Report Pro-Forma

1.	Departmental fraud reference number (unique identifier)	(will be completed once forwarded to DAERA)
2.	Department	(will be completed once forwarded to DAERA)
3.	Name of body (e.g. specific Board, Trust, NDPB, Agency etc.)	AFBI
4.	Specific location of fraud (e.g. name of school, name of depot etc.)	
5.	Date fraud or suspected fraud discovered	
6.	Is the case being reported as actual, suspected or attempted fraud?	
7.	Type of fraud?	
8.	What was the cause of the fraud?	
9.	Brief outline of case	
10.	Amount of lost or estimated value?	
11.	How was the fraud discovered?	
12.	Who perpetrated the fraud?	
13.	Has PSNI been notified?	Yes/ No
14.	Any other action taken so far?	
15.	Please give contact details for this fraud in case follow-up is required	Name: Telephone: Email:

## **Notes**

### **1. Types of fraud**

- Grant related
- Theft of assets (please state type of asset e.g. cash, laptop, oil, tools, camera)
- Payment process related
- Income related
- Pay or pay related allowances
- Travel and subsistence
- Pension fraud
- Contractor fraud
- Procurement fraud
- False representation
- Failure to disclose information
- Abuse of position
- Other (please specify)

### **2. Causes of fraud**

- Absence of proper controls
- Failure to observe existing controls
- Opportunistic
- Unknown

### **3. Means of discovery of fraud**

- Normal operation of control procedures
- Whistleblowing (internal or external)
- Internal Audit
- External
- Computer analysis/National Fraud Initiative
- Other means (please specify)

### **4. Perpetrators of Fraud**

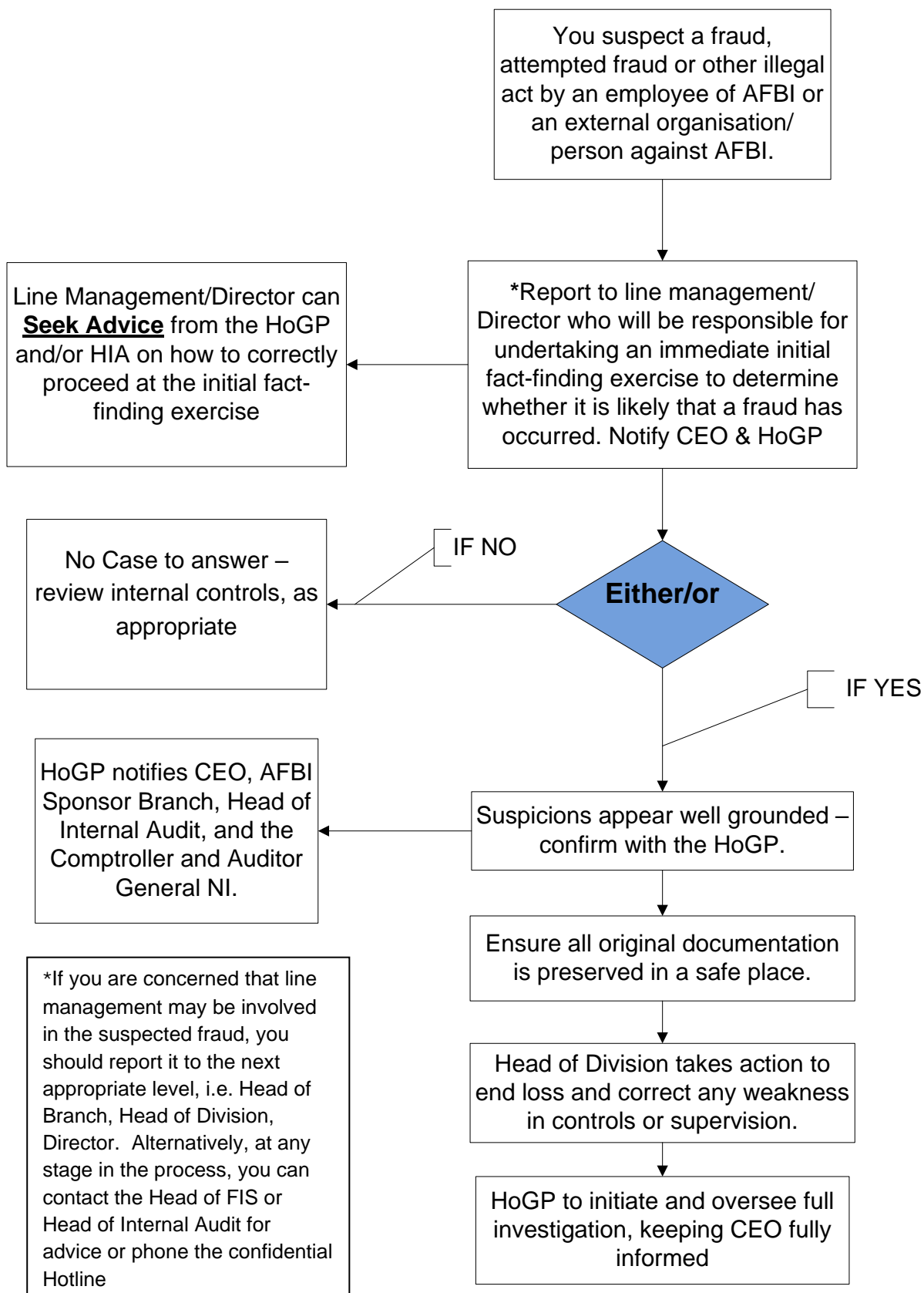
- Internal staff member
- Contractor
- Funded body/grant applicant
- Other third party (please specify)
- Collusion between internal and external parties
- Too early to determine
- Unknown

### **5. Other actions taken**

- Controls improved
- Control improvements being considered
- Too early to determine

- No action possible
- Disciplinary action
- Prosecution

## APPENDIX G – Reporting Fraud/Suspected Fraud



## APPENDIX H – Contact Details

Designation	Telephone Number
Head of Governance and Performance	028 90 255494
AFBI Chief Executive	028 90 255687

## APPENDIX I – Memorandum of Understanding

# Memorandum of Understanding between the Northern Ireland Public Sector and the Police Service of Northern Ireland (PSNI)



## 1. INTRODUCTION

This memorandum sets out a basic framework for the working relationship between the Northern Ireland Public Sector (as defined below) and the Police Service of Northern Ireland, in respect of the investigation and prosecution of suspected fraud cases.

It is recognised and accepted by the public sector bodies participating in this Memorandum, as listed in Annex A and by the PSNI that this Memorandum shall not be regarded as a contract and does not create any rights, liabilities, or obligations which would have a binding effect in law. It is intended to record the agreed best practice to be followed, but is purely advisory and does not itself seek to impose any obligations or restrictions beyond those contained in the relevant applicable legislation.

## 2. THE NORTHERN IRELAND PUBLIC SECTOR BODIES COVERED BY THIS MEMORANDUM

The NICS departments are responsible for all matters, which would be devolved to the Assembly if suspension were lifted e.g. health, social security, urban regeneration, arts and leisure, agriculture etc. The NICS departments are not responsible for matters such as policing and organised crime, security policy, prisons, criminal justice, international relations, taxation, national insurance, regulation of financial services and the regulation of telecommunications and broadcasting which are excepted or reserved matters and are therefore dealt with by the Northern Ireland Office (NIO). Separate arrangements apply to NIO responsibilities.

NICS departments may also have a number of Agencies and sponsored bodies e.g. Non Departmental Public Bodies (NDPBs), Health Trusts, Councils etc. established to undertake the executive functions of government as distinct from policy advice. Agencies are either Supply-financed or financed through a trading fund. NDPBs can be financed by a grant or grant-in-aid, levies, loans from the Northern Ireland Consolidated Fund (NICF) or in the case of small ones such as advisory bodies, directly from the sponsor department's

Estimate. The Health Boards and Trusts are funded by the Department of Health, Social Services and Public Safety and the Councils through the rates and grants from the Department of the Environment.

Given the nature of this Memorandum it is expected that it will apply to the Northern Ireland Public Sector defined to include all the bodies above.

A full list of the Public Sector bodies covered by this memorandum can be found at Annex A. This list may be subject to change e.g. as a result of Machinery of Government Changes such as the Review of Public Administration.

### **3. THE POLICE SERVICE OF NORTHERN IRELAND (PSNI)**

The PSNI was established in November 2001 as a result of the recommendations of the Independent Commission on Policing in Northern Ireland, which was set up as a result of the Belfast Agreement.

The purpose of the PSNI is to make Northern Ireland safer for everyone through professional, progressive policing upholding the values of:

- Honesty and openness;
- Fairness and courtesy;
- Partnerships, performance, professionalism; and
- Respect for the rights of all.

Increasingly the PSNI has been concerned to promote a fraud prevention strategy in the Public and Private Sectors.

#### 4. WHAT IS FRAUD?

At the time of writing there is no precise legal definition of fraud and for practical purposes, fraud may be defined as “causing loss or making a gain at the expense of someone by dishonest means”.<sup>1</sup> However, fraudulent behaviour encompasses a variety of offences such as theft, false accounting and bribery and corruption. However, the lack of a precise definition of fraud leaves room for interpretation and hence the Law Commission prompted the Home Office to introduce the Fraud Bill, which is now before Parliament. The bill will, for the first time, define fraud in English law.

#### 5. STATEMENT OF INTENT

This memorandum aims to set out a framework to ensure appropriate action is taken by the public sector organisations stipulated at Annex A, in line with DFP guidelines to deal with cases of suspected fraud as set out in Chapter 5 of Government Accounting Northern Ireland (GANI) and other guidance issued by DFP and that actions throughout the investigative process are conducted in accordance with the Police and Criminal Evidence (Northern Ireland) Order 1989 (PACE) where appropriate.

It also provides for the exchange of relevant information between the two parties and seeks to ensure that such disclosure of information to the other is in a timely manner and complies with any relevant legislation.

A list of departmental contacts, having responsibility for the effective working of this MOU, is contained in Annex B and this will need to be augmented in those organisations covered by this memorandum by equivalent contact points<sup>2</sup>.

<sup>1</sup> Fraud Review, July 2006: 24

<sup>2</sup> These contacts are for the operation of the MOU and not intended to override operational contacts already working within some departments/bodies or appointed by them to work on their behalf.

The working relationship between the NI Public Sector and the PSNI through nominated contact points is designed to:

- Facilitate the prompt and effective processing of investigations in cases of suspected fraud;
- Ensure that cases of suspected fraud are referred promptly to agreed PSNI contact points and in the agreed format (Annex D);
- Ensure that all investigative work undertaken by public bodies prior to formal referral to PSNI has been fully compliant with the Police and Criminal Evidence (Northern Ireland) Order 1989 (PACE);
- Provide a consistent approach to those cases referred to the PSNI for investigation;
- Provide the PSNI with nominated contacts within Public Sector bodies for the conduct of fraud investigations;
- Ensure that information passing between the PSNI and the NICS is dealt with confidentially and processed in accordance with the terms of this memorandum<sup>3</sup> and any legislative requirements; and
- Develop the concept of mutual aid.

## 6. OPERATING PROTOCOLS

### *Referrals*

Public bodies should liaise with the PSNI Fraud Unit as appropriate, making reference to the guidance set out in the Management Checklist, issued by DFP under cover of DAO (DFP) 12/06.

Subject to the Acceptance Criteria as outlined at Annex C the public

<sup>3</sup> Where this does not conflict with any existing arrangements between a particular body and the PSNI, in which case, the existing arrangements should prevail

body will forward an Evidence Pack to the PSNI Fraud Unit.

On receipt of the Evidence Pack (see Annex D) the PSNI Fraud Unit will assess the case and subject to the outcome of the assessment process the PSNI Fraud Unit will:

1. Accept the case for investigation;
2. Refer the case to PSNI district command for investigation;
3. Refer the case to originating public sector body for further enquiry/action/information.

Having accepted a case for investigation the PSNI and Public Sector Body concerned, should agree at the outset, arrangements for monitoring progress on the case.

## **7. PERIOD OF OPERATION**

This memorandum takes effect from 30 October 2006.

The parties will be required to give 6 months notice, in writing, to terminate the memorandum.<sup>4</sup>

## **8. REVIEW OR VARIATION OF MEMORANDUM**

This memorandum will be formally reviewed each year, however, either party may ask for a review at any time. Any variations will be recorded and the revisions will be issued by the Memorandum Co-ordinators (see paragraph10).

This memorandum may have to be reviewed or suspended in the event of an emergency involving the implementation of either party's Business Contingency Plans.

---

<sup>4</sup> This requirement can be relaxed in exceptional circumstances with the agreement of both parties

**9. MOU LIASON ARRANGEMENTS AND DISPUTES PROCEDURES**

Close liaison is essential to ensure the effective and economic delivery of the services specified in this memorandum. Liaison should be through the nominated contacts listed in Annex B for this purpose.

Disputes should be resolved at operational level. Those that cannot be resolved locally in terms of the operation of this MOU should be escalated to the Fraud Forum for resolution via the departmental contacts listed in Annex B.

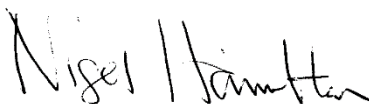
**10. MEMORANDUM CO-ORDINATORS**

The Fraud Forum (representing the NICS departments, their agencies and sponsored bodies) and the PSNI will appoint Memorandum Co-ordinators who will be responsible for monitoring the operation of the memorandum and making any changes to it. The Co-ordinators are:

**NI Public Sector** Head of Accountability and Accountancy Services  
Division in DFP

**PSNI** Head of Fraud Unit

**This Memorandum is signed by:**



**Head of the Northern Ireland Civil Service  
(NI Public Sector)**



**Chief Constable  
(PSNI)**

**Date: 30 OCTOBER 2006**

**ANNEX A****Departments, Agencies, NDPBs, Councils and Health Boards and Trusts covered by this memorandum**

Agri-food and Biosciences Institute  
Air Route Development (Northern Ireland) Limited  
Arts Council of Northern Ireland  
Belfast Education and Library Board  
Construction Industry Training Board  
Council for Catholic Maintained Schools  
Department for Employment and Learning  
Department for Regional Development  
Department for Social Development  
Department of Agriculture and Rural Development  
Department of Culture, Arts and Leisure  
Department of Education  
Department of Enterprise, Trade and Investment  
Department of Finance and Personnel  
Department of Health, Social Services and Public Safety  
Department of the Environment  
Disability Living Allowance Advisory Board for Northern Ireland  
Driver & Vehicle Licensing  
Driver and Vehicle testing Agency  
Economic Research Institute of Northern Ireland  
Employment Medical Advisory Service  
Enterprise Ulster  
Environment & Heritage Service  
Fisheries Conservancy Board  
Forest Service  
General Consumer Council for Northern Ireland  
Health and Safety Executive for Northern Ireland  
Health Estates  
Illex Urban Regeneration Company Limited  
Invest Northern Ireland  
Labour Relations Agency  
Laganside Corporation  
Land Registers of NI  
Livestock and Meat Commission  
Local Government Staff Commission for Northern Ireland  
Mental Health Commission for Northern Ireland

National Museums and Galleries of Northern Ireland  
North Eastern Education and Library Board  
Northern Ireland Authority for Energy Regulation  
Northern Ireland Blood Transfusion Service (Special Agency)  
Northern Ireland Child Support Agency  
Northern Ireland Council for the Curriculum, Examinations and Assessment  
Northern Ireland Events Company  
Northern Ireland Film & Television Commission  
Northern Ireland Fire and Rescue Service  
Northern Ireland Fishery Harbour Authority  
Northern Ireland Guardian ad Litem Agency  
Northern Ireland Health Promotion Agency  
Northern Ireland Housing Executive  
Northern Ireland Local Government Officers' Superannuation Committee  
Northern Ireland Medical and Dental Training Agency  
Northern Ireland Museums Council  
Northern Ireland Practice and Education Council for Nursing and Midwifery  
Northern Ireland Regional Medical Physics Agency  
Northern Ireland Social Care Council  
Northern Ireland Statistical & Research Agency  
Northern Ireland Tourist Board  
Northern Ireland Transport Holding Company  
Office of the First Minister and Deputy First Minister  
Ordnance Survey of Northern Ireland  
Planning Service  
Public Records Office of Northern Ireland  
Rate Collection Agency  
Rent Assessment Panel  
Rivers Agency  
Roads Service  
Rural Development Council  
Social Security Agency  
South Eastern Education and Library Board  
Southern Education and Library Board  
Sports Council for Northern Ireland  
Staff Commission for Education and Library Boards  
Strategic Investment Board Limited  
The Commissioner for Children and Young People for Northern Ireland  
The Equality Commission for Northern Ireland  
The Governors of the Armagh Observatory and Planetarium  
Ulster Supported Employment Limited  
Valuation & Lands Agency  
Vaughan Charity

Water Service  
Western Education and Library Board  
Youth Council for Northern Ireland

### **City, District & Borough Councils**

Antrim Borough Council  
Ards Borough Council  
Armagh City and District Council  
Ballymena Borough Council  
Ballymoney Borough Council  
Banbridge District Council  
Belfast City Council  
Carrickfergus Borough Council  
Castlereagh Borough Council  
Coleraine Borough Council  
Cookstown District Council  
Craigavon Borough Council  
Derry City Council  
Down District Council  
Dungannon and South Tyrone Borough Council  
Fermanagh District Council  
Larne Borough Council  
Limavady Borough Council  
Lisburn City Council  
Magherafelt District Council  
Moyle District Council  
Newry and Mourne District Council  
Newtownabbey Borough Council  
North Down Borough Council  
Omagh District Council  
Strabane District Council

### **Health & Social Services Trusts**

Altnagelvin Hospitals Health and Social Services Trust  
Armagh and Dungannon Health and Social Services Trust  
Belfast City Hospital Health and Social Services Trust  
Causeway Health and Social Services Trust  
Craigavon Area Hospital Group Health and Social Services Trust  
Craigavon and Banbridge Community Health and Social Services Trust

Down Lisburn Health and Social Services Trust  
Foyle Health and Social Services Trust  
Green Park Health and Social Services Trust  
Homefirst Community Health and Social Services Trust  
Mater Infirmorum Hospital Health and Social Services Trust  
Newry and Mourne Health and Social Services Trust  
North and West Belfast Health and Social Services Trust  
Northern Ireland Ambulance Service Health and Social Services Trust  
Northern Ireland Central Services Agency for the Health and Social Services  
Northern Ireland Health and Personal Social Services Regulation and Quality  
Improvement Authority  
Royal Group of Hospitals and Dental Hospital Health and Social Services  
Trust  
South and East Belfast Health and Social Services Trust  
Sperrin Lakeland Health and Social Services Trust  
Ulster Community and Hospitals Health and Social Services Trust  
United Hospitals Health and Social Services Trust

#### **Health and Social Services Boards**

Eastern Health and Social Services Board  
Western Health and Social Services Board  
Northern Health and Social Services Board  
Southern Health and Social Services Board

## ANNEX B

**DEPARTMENTAL & PSNI CONTACTS****1. DEPARTMENTAL CONTACTS FOR THE OPERATION OF THE MOU**

DEPARTMENT	NAME OF CONTACT	CONTACT DETAILS
DARD	Thomas McCauley	<a href="mailto:Thomas.McCauley@dardni.gov.uk">Thomas.McCauley@dardni.gov.uk</a>
DCAL	Michelle Estler	<a href="mailto:Michelle.Estler@dcalni.gov.uk">Michelle.Estler@dcalni.gov.uk</a>
DE	Paul Wright	<a href="mailto:Paul.Wright@deni.gov.uk">Paul.Wright@deni.gov.uk</a>
DEL	Eamon Campbell	<a href="mailto:Eamon.Campbell@delni.gov.uk">Eamon.Campbell@delni.gov.uk</a>
DETI	Terry Coyne	<a href="mailto:Terence.Coyne@detini.gov.uk">Terence.Coyne@detini.gov.uk</a>
DFP	Michael Matthews	<a href="mailto:Michael.Matthews@dfpni.gov.uk">Michael.Matthews@dfpni.gov.uk</a>
DHSSPS	Sandra Lowe	<a href="mailto:Sandra.Lowe@dhsspsni.gov.uk">Sandra.Lowe@dhsspsni.gov.uk</a>
DOE	Peter Aiken	<a href="mailto:Peter.Aiken@doeni.gov.uk">Peter.Aiken@doeni.gov.uk</a>
DRD	Stephen McKillop	<a href="mailto:Stephen.McKillop@drdni.gov.uk">Stephen.McKillop@drdni.gov.uk</a>
DSD	Eamonn McCarron	<a href="mailto:Eamonn.Mccarron@dsdni.gov.uk">Eamonn.Mccarron@dsdni.gov.uk</a>
OFMDFM	Deirdre Griffith	<a href="mailto:Deirdre.Griffith@ofmdfmni.gov.uk">Deirdre.Griffith@ofmdfmni.gov.uk</a>

**2. PSNI CONTACTS FOR THE OPERATION OF THE MOU**

DEPARTMENT/UNIT	NAME OF CONTACT	CONTACT DETAILS
PSNI, Fraud Unit	John Cherry	<a href="mailto:John.Cherry@psni.pnn.police.uk">John.Cherry@psni.pnn.police.uk</a>
PSNI, Fraud Unit	Katherine Montgomery	<a href="mailto:Katherine.Montgomery@psni.pnn.police.uk">Katherine.Montgomery@psni.pnn.police.uk</a>

**ANNEX C****REFERRAL TO PSNI: ACCEPTANCE CRITERIA**

1. These criteria set out the conditions necessary for a suspected fraud case to be referred to the PSNI. **However, the decision to accept a case for investigation rests fully with the PSNI who will provide their decision in writing.**
  - It must be established that there are reasonable grounds to believe that a criminal offence has been committed.
  - Deliberate criminal intent needs to be clearly defined. The fraud needs to be more than an error or omission.
  - The allegations should concern recent events and should not have become stale by reason of age. Incidents, which are over two years old before discovery, need to be judged individually on their merits, including availability of documentary evidence and the reliability of witness evidence.
  - To comply with the rules governing disclosure, the department/body will identify and preserve all original documents and other exhibits relating to any intended complaint.
  - The department/body should be prepared to supply all original relevant documents and exhibits to the police if an investigation is accepted and commenced. Such evidential material should be securely held, in accordance with PACE provisions, before formal hand over to the PSNI.

**ANNEX D****PSNI AGREED FORMAT OF EVIDENCE PACK**

1. Evidential packages should contain a detailed summary of all relevant information surrounding the allegations made. This should include the nature of the allegations against the suspect, including the full name, address and date of birth of the suspect.
2. The package should also include: -
  - All available details of any other parties suspected of involvement in the alleged fraud, including the reasons for the suspicions;
  - A brief summary of the allegations including estimated values of alleged crime and relevant dates;
  - A full description of the nature of the crime and the circumstances surrounding it. This should include full details of any investigations already undertaken by the department/body or anyone acting on their behalf;
  - Copies of all relevant documents, each individually numbered and identified in the summary;
  - Copies of all statements obtained from suspects;
  - Names and addresses of all witnesses identified at the time of reporting to the police, including copies of any statements;
  - Any police reference numbers, which may already apply to any part of the case; and
  - A name and contact point.

