

# **ANTI-FRAUD POLICY**

# CONTENTS

- 1. INTRODUCTION 3
- 2. WHAT IS FRAUD? 3
- 3. MANAGING THE RISK OF FRAUD 5
- 4. RESPONSIBILITIES 5
- 5. REPORTING FRAUD 6
- 6. ETHICS AND CONDUCT OF STAFF 7
- 7. DISCIPLINARY ACTION 7
- 8. REVIEW 7
- APPENDIX A — FRAUD INDICATORS 8

# 1. INTRODUCTION

- 1.1 NILGOSC requires 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 there is a continuing need to raise staff awareness about fraud prevention and detection.
- 1.2 NILGOSC has a zero tolerance towards fraud and is committed to reducing the opportunity for fraud to the lowest possible level of risk. Any cases of detected or suspected incidents of fraud will be thoroughly investigated and dealt with appropriately.
- 1.3 The purpose of this policy is to set out the roles and responsibilities of NILGOSC staff regarding the prevention, detection and response to fraud. The procedures to be followed in the event of a fraud being detected or suspected are detailed in the Fraud & Corruption Response Plan. Both documents should be referred to and applied where a fraud relating to NILGOSC is detected or suspected.

## 2. WHAT IS FRAUD?

### 2.1 Legal definition of fraud

- 2.1.1 The Fraud Act 2006 came into effect in January 2007 and provides a legal definition of fraud. The Act states that fraud can be committed in three ways:
  - false representation
  - failure to disclose information where there is a legal duty to disclose
  - abuse of position.
- 2.1.2 The Act also creates three new offences to assist in the fight against fraud. These include obtaining services dishonestly; of possessing, making and supplying articles for use in frauds; and fraudulent trading.
- 2.1.3 The Act further requires that the person committing the fraud must do so with the intention of making a gain or causing loss or risk of loss to another. The key factor to consider is the intention of the individual concerned, not whether a gain or loss has actually taken place.
- 2.1.4 While the Act provides a legal definition of fraud, the general public consider fraud in its widest sense in relation to theft, false accounting, bribery and corruption, conspiracy to defraud, money laundering, etc. The Bribery Act 2010 came into force on 1 July 2011 and 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. Cases of bribery and corruption will be dealt with under NILGOSC's Anti-Bribery Policy.

### 2.2 Internal Fraud

- 2.2.1 Internal fraud (also referred to as staff fraud or insider fraud) is fraud committed against an organisation by someone employed by the organisation. Internal fraud can range from minor thefts of assets, expense claim inflation to major diversion of funds, accounting frauds or exploitation of payroll or service user data. A person employed by an organisation includes contracted employees, temporary staff, agency workers and contractors<sup>1</sup>.

### 2.3 How fraud occurs

- 2.3.1 The fraud triangle is used by fraud experts to explain why fraud happens, when the three following elements combine<sup>2</sup>:
  - Pressure – motivation or incentive to commit fraud
  - Opportunity – ability to carry out fraud
  - Rationalisation- justification of dishonest actions

<sup>1</sup> Internal Fraud Risks, Northern Ireland Audit Office, 2022

<sup>2</sup> Ibid

2.3.2 Types of fraud which may be relevant to NILGOSC include but are not limited to:

- receipt of pension benefits to which no entitlement exists
- receipt of income (most common), i.e. retention and misappropriation of cash
- diversion of funds
- expenses claims
- purchase and payments systems
- misuse of the organisation credit card
- false wage, salary and pension claims
- theft of equipment and stores
- use of supplies/equipment/devices for personal projects
- false accounting
- suppression of documents
- misuse of computer
- cyber fraud e.g. phishing emails
- working elsewhere while off sick
- use official working hours to conduct personal business
- use of false identity/documents/qualifications by prospective employee
- use of false identity by scheme member/beneficiary
- fraud in the procurement process where an involved staff member favours the business of a family member or friend
- Fraud in the recruitment process where an involved staff member favours an application who is a family member or friend
- Where an interest is not declared by a staff or Committee member in a situation where they could use their professional position for personal gain

## **2.4 Detection of fraud**

2.4.1 It has been observed that certain changes within an organisation or the introduction of a new work practice or policy can trigger certain people into committing fraud. Some of the causes of concern are:

- changing culture and environment
- changing organisational structures
- changing technology
- lack of fraud or corruption consciousness in management.

2.4.2 Cases of fraud or corruption have been discovered not because of any great in-depth investigation but rather because the perpetrators drew attention to themselves by their actions, behaviour and/or attitude. Some of the items to watch are:

- perpetrator living beyond their means
- overwhelming desire for personal gain
- high personal debts
- too close an association with customers
- extreme gambling habits
- undue family or peer pressure
- the feeling that pay was not commensurate with responsibility
- a "wheeler-dealer" attitude
- a strong challenge to beat the system.

2.4.3 Fraud indicators are clues or hints that a closer look should be made at an individual, area or activity within an organisation. To spot fraud indicators in individual areas or activities it is important that accepted practices have been established for the area or activity under review and that reviewers are familiar with them. Examples of issues that could be investigated to ensure fraud is not taking place can be found in Appendix A.

# 3. MANAGING THE RISK OF FRAUD

- 3.1 Fraud risk is the vulnerability or exposure NILGOSC has towards fraud and irregularity. It combines the probability of fraud occurring and the corresponding impact measured in monetary and reputational terms.
- 3.2 In respect of fraud risks, prevention is preferable to detection and the strongest defence is a sound system of internal control. NILGOSC manages the risk of fraud through its risk management, governance and internal control processes in order to improve controls in problem areas and be pro-active in detection. Fraud risk is included in NILGOSC's risk register, which is reviewed on a quarterly basis by the Senior Management Team. Any areas of concern are reported to the Audit & Risk Assurance Committee. The internal audit function also provides a level of assurance against the system of internal control operating within NILGOSC.
- 3.3 NILGOSC recognises the increasing threat of cyber-attack for organisations. Cyber fraud can come in various forms and relates to any criminal act dealing with computers, networks or through the internet, with the intention of making a gain or causing a risk or actual loss to another. NILGOSC has controls and measures in place to mitigate against the risk of a cyber attack. These are set out in NILGOSC's Information Security Policy and the risks and controls are monitored on an ongoing basis by the IT Team. Since 2020 NILGOSC has participated in a government backed scheme with the Cyber Security Centre for Northern Ireland. NILGOSC has attained the Cyber Essentials Plus accreditation each consecutive year since.
- 3.4 NILGOSC also takes part in data matching exercises through the National Fraud Initiative and with the General Registrar's Office for Northern Ireland. This compares information held by different organisations to identify potentially fraudulent claims and overpayments. NILGOSC also engages with a third party provider to provide a tracing service to match data for members who are not traceable.

# 4. RESPONSIBILITIES

- 4.1 Fraud can flourish where there are deficiencies in management control systems so it is the responsibility of management to take all reasonable steps to limit the opportunities for fraud to occur within NILGOSC through a sound system of internal controls. In line with Annex 4.7 in Managing Public Money Northern Ireland (MPMNI) specific responsibilities in relation to fraud are set out below:
- 4.1.1 The **Accounting Officer** has overall responsibility for:
- developing and maintaining an effective system of internal controls to prevent fraud or corruption and to ensure that if it does occur it will be detected promptly
  - carrying out vigorous, prompt and independent investigations if fraud or corruption occurs
  - taking appropriate legal and/or disciplinary action against managers where management failure has contributed to the occurrence of fraud or corruption
  - where incidents of fraud or corruption have been identified, making the necessary changes to the systems and procedures to ensure that similar breaches will not happen again
  - establishing systems for recording and subsequently monitoring all discovered cases of fraud.
- 4.1.2 Although the Accounting Officer bears overall responsibility and is liable to be called to account for specific failures, these responsibilities are shared with the senior management team, who have responsibility for managing the internal controls within their respective areas and providing assurance on the effective operation of those controls to the Accounting Officer.
- 4.1.3 The **Head of Governance & Human Resources** is responsible for:
- establishing an effective anti-fraud policy and fraud response plan;
  - establishing appropriate mechanisms for reporting fraud risk issues and reporting significant incidents of fraud to the Accounting Officer and Department as appropriate;
  - liaising with the Audit & Risk Assurance Committee; and
  - raising staff awareness about the Anti-Fraud Policy and ensure that staff know what their responsibilities are in relation to detecting and preventing fraud.

#### 4.1.4 **Managers** are responsible for:

- Identifying and assessing the risks involved in the operations, systems and procedures they are responsible for;
- developing and maintaining effective internal controls to prevent and detect fraud or corruption within their area of responsibility;
- reviewing and testing the internal control systems to ensure that controls are being complied with and that the systems continue to operate effectively;
- providing regular assurance to the Accounting Officer on the effectiveness of the controls within their area of responsibility.
- implementing new controls when a fraud has been detected to reduce the risk of it being repeated;
- ensuring compliance with the Anti-Fraud Policy and Fraud & Corruption Response Plan within their area of responsibility; and
- initiating appropriate action when staff fail in their responsibilities regarding fraud.
- initiating legal and/or disciplinary action against perpetrators of fraud, where appropriate.

#### 4.1.5 **Every member of staff** is responsible for:

- acting with propriety in the use of official resources and in the handling and use of public funds whether they are involved with cash or payments systems, receipts or dealing with contractors or suppliers;
- alerting their line manager where they believe the opportunity for fraud or corruption exists, for example due to poor internal controls or procedures;
- reporting details immediately to their line manager or next most senior manager if they suspect that a fraud or corruption has been committed or see any suspicious acts or events; and
- making available all relevant information and co-operating fully with any investigation.

#### 4.1.6 **Internal Audit** is responsible for:

- delivering an opinion to the Accounting Officer on the effectiveness of the controls for managing the risk of fraud and ensuring that NILGOSC promotes an anti-fraud culture;
- assisting in the deterrence and prevention of fraud by examining and evaluating the effectiveness of controls commensurate to the level of fraud risk; and
- ensuring that management has reviewed its risk exposures and identified the possibility of fraud as a business risk.

## 5 REPORTING FRAUD

5.1 NILGOSC has in place a Fraud & Corruption Response Plan which sets out how to report suspicions and how investigations will be conducted. The Fraud & Corruption Response Plan covers the following areas:

- who to report to and when;
- how to conduct preliminary enquiries;
- how to secure evidence;
- when and how to contact the police;
- how to prevent losses; and
- how to initiate recovery action

5.2 All staff should familiarise themselves with the guidance contained within the Fraud & Corruption Response Plan, which is available on the Intranet. The Fraud & Corruption Response Plan should be referred to and applied step-by-step when a fraud is suspected or detected.

5.3 Alternatively staff may wish to raise such matters through NILGOSC's Raising Concerns Policy, which sets out the procedures and protections which will apply to staff making such disclosures.

5.4 Committee members who wish to raise concerns about any suspected or actual attempts of fraud should report these to the Chairperson and/or the Secretary/Deputy Secretary. If this is not deemed appropriate, then the Committee member should refer to NILGOSC's Raising Concerns Policy to report their concerns externally.

- 5.5 Third parties, contractors or members of the public who wish to report any suspected or actual attempts of fraud relating to NILGOSC, should also raise their concerns through NILGOSC's Raising Concerns Policy.
- 5.6 Alternatively, incidents can be reported confidentially via the NILGOSC **Fraud and Corruption Hotline (Telephone: (028) 9076 4198 Extension: 459)**. All concerns raised will be investigated in line with the Raising Concerns Policy, with reference to the Fraud & Corruption Response Plan.

## 6. ETHICS AND CONDUCT OF STAFF

- 6.1 Staff owe a duty of care to NILGOSC and to the public at large. As stewards of public funds, staff must have and be seen to have high standards of honesty, propriety and integrity in the exercise of their duties. Accordingly, staff should not accept gifts, hospitality or benefits of any kind from a third party which would, or could be seen to, compromise their integrity. Staff should refer to the Staff Code of Conduct, the Purchasing Policy, the Conflicts of Interest Policy and the Acceptance of Gifts, Services and Hospitality Policy for further advice and information.

## 7. DISCIPLINARY ACTION

- 7.1 In the course of any investigation the facts may support disciplinary action if the fraud or corruption has been undertaken by a member of staff. In all cases of proven fraud, disciplinary action will be taken to its fullest conclusion.
- 7.2 If the investigation uncovers a failure of supervision, disciplinary action may be taken against those responsible.
- 7.3 In addition to disciplinary action every effort will be made to recoup loss of funds.

## 8. REVIEW

- 8.1 NILGOSC will review and update its Anti-Fraud Policy and the Fraud & Corruption Response Plan every three years, or more often as required. The next review will be due in July 2026.
- 8.2 Any queries in relation to the Anti-Fraud Policy or the Fraud & Corruption Response Plan should be referred to the Governance Team at [governance@nilgosc.org.uk](mailto:governance@nilgosc.org.uk).

# APPENDIX A – 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, fails to take leave, managers by-passing subordinates, subordinates by-passing managers, living beyond means, regular working of long hours, job dissatisfaction/unhappy employee, secretiveness or defensiveness).
- Unrecorded transactions or missing records (e.g. invoices, 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.
- 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 area

## Document Control

### Document Details

REFERENCE	<b>ANTI FRAUD POLICY</b>
DATED	<b>27/11/2023</b>
PREPARED BY	<b>Catherine Whyte</b>
AUDIENCE	<b>All staff</b>

### Document History

VERSION	DATE	SUMMARY OF CHANGES	AUTHOR
<b>2.0</b>	27/11/2023	<ul style="list-style-type: none"><li>• a definition of internal fraud has been added.</li><li>• types of fraud have been added which may be relevant to NILGOSC.</li><li>• reference to NILGOSC's Conflicts of Interest Policy.</li><li>• reference to the Cyber Essentials plus accreditation.</li></ul>	Catherine Whyte