General Teaching Council for Northern Ireland

Promoting Teacher Professionalism

Anti-fraud and Bribery Policy

Version 1.3 February 2024

Review Date: December 2026

Contents

Introduction

There is a continuing need to raise staff awareness of our responsibility to safeguard members' resources against the risk of fraud. This document sets out GTCNI's Anti-Fraud and Bribery Policy. A separate Fraud Response Plan details those actions which must be taken by Business Areas in the event of a fraud, attempted fraud or irregular activity being suspected.

Fraud is not a victimless crime. We are entrusted with members' money, and we must look after it in the same way that we look after our own. So we must all be aware of:

- what constitutes fraud;
- the potential for fraud;
- steps to prevent fraud in the first instance, and
- what to do in the event of fraud or if we suspect fraud has occurred

The Anti-Fraud and Bribery Policy sets out the organisation's commitment to dealing with allegations of irregularities, fraud and bribery.

GTCNI has a zero tolerance policy in relation to fraud, bribery and corruption and is committed to acting fairly and with integrity in all of its business dealings and relationships and implementing and enforcing effective systems to counter bribery.

By identifying areas where the risk of fraud exists, detecting fraud which has already occurred, taking firm action against the perpetrators and designing systems to prevent the occurrence of fraud on all its forms, the Anti-Fraud and Bribery Policy aims to develop a culture across GTCNI which raises the awareness of the risks and consequences of fraud and taking or offering of bribes. It provides a framework for promoting GTCNI's policies and measures to prevent and detect fraud.

The procedure for staff to report concerns is known as a Fraud and Bribery Response Plan. It outlines how allegations of fraud and bribery should be made and what steps the organisation will take when dealing with them.

All cases of suspected or actual fraud should be reported immediately to the Head of Corporate Services who will advise management on what steps to take next.

If staff become aware of wrongdoing there may be some circumstances where they are afraid to voice their concern, especially if the case involves a more senior officer. The Public Interest Disclosure (Northern Ireland) Order 1998 protects individuals from

workplace retributions for raising a genuine concern whether a risk to the public purse or other wrongdoing. GTCNI has a Whistleblowing Policy (Raising Concerns) to assure you that it is safe to speak up if you are concerned about something. Please ensure that you familiarise yourself with your anti-fraud responsibilities and the steps which you must take in the event of fraud or suspected fraud (see the Fraud Response Plan).

Our Statement of Intent

As outlined in GTCNI's Whistleblowing Policy and Protocol, it is the responsibility of public bodies to serve the public interest and therefore we must discharge our duties in line with our values.

Openness We will promote a culture of openness and will be transparent and honest in our dealings with the public, our partners and colleagues.

Respect We will listen to and respect those we serve, as well as each other and will recognise effort, achievement and contribution.

Reflection We will be a learning organisation, reflecting and taking on board the lessons learned from our own experiences and from comparable organisations.

Responsibility We will act responsibly and acknowledge that our actions will impact on others. We will be helpful, conscientious, reliable and accountable for all our actions.

Excellence We will strive for quality in everything we do. We will behave professionally and take pride and ownership for everything we say and do.

Equality We will strive for equality in everything we do. We will behave professionally and take pride and ownership for everything we say and do. We will promote equality of opportunity through our employment practices, service delivery and engagement activities.

The aim of this guidance is to promote high standards of governance within GTCNI and promote the key characteristics of public life, as defined by the **Nolan Principles**. These seven principles underpinning public life are: Selflessness; Integrity; Objectivity; Accountability; Openness; Honesty; and Leadership.

Our People Strategy

GTCNI's Anti-fraud and Bribery Policy, which should be read in conjunction with the Whistleblowing and Raising Concerns at Work Policy, aims to have a well-led, high-performing and outcomes-focused GTCNI, which is a great place to work, where everyone can reach their full potential, and can do so in an environment where they are supported by well-documented policies and clear supportive procedures on all aspects of work, including a requirement for all employees 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 hence must be a concern to all employees.

Our ambition is long-term, but to achieve the outcomes we want we have identified priorities (goals and work-streams) which we will act on now.

A well-led GTCNI	*A high-performing GTCNI*	*An Outcomes-focused GTCNI*	*An inclusive GTCNI in which diversity is truly valued – a great place to work*
• Improve how we engage and communicate with people across the organisation about issues that affect them	• Improve how we manage performance through regular and timely feedback mechanisms and appropriate guidance	• Build career progression that develops breadth of experience and depth of expertise	• Deliver evidence-based interventions and targeted action to drive balance and inclusion in terms of gender, LGB&T, minority ethnic and disability
• Build the capacity of supervisors, line managers and leaders across the organisation	• Deliver a GTCNI-wide approach to strategic workforce planning and improve recruitment and vacancy management	• Improve how we engage with staff and communicate with them about their contribution to delivery of outcomes	• Ensure our people have working environments that are conducive to them performing at their best
• Provide effective tools for supervisors, line managers and leaders, including streamlined and practical people policies, processes, guidance and training	• Increase the use of new and flexible ways of working		

Policy Scope

This policy applies to all permanent and temporary employees of GTCNI (including any of its intermediaries, subsidiaries or associated companies), It also applies to any individual or corporate entity associated with the company or who performs functions in relation to or for and on behalf of GTCNI, including, but not limited to, governance bodies, agency workers, casual workers, contractors, consultants, seconded staff, agents, suppliers and sponsors “associated persons”. All employees and associated persons are expected to adhere to the principles set out in this policy.

Promoting an Anti-Fraud Culture

GTCNI promotes an anti-fraud culture through the following:

- any allegation of fraud (anonymous or otherwise) will be investigated;
- consistent handling of cases without regard to position held or length of service;

- consideration of whether there have been failures of supervision. Where this has occurred disciplinary action may be initiated against those responsible;
- losses resulting from fraud will be recovered, if necessary, through civil action;
- in general all frauds will be publicised as a deterrent;
- by regularly circulating its anti-fraud policy statement;
- participation in the National Fraud Initiative whereby data is matched to combat fraud in the public sector; and
- prominently displaying the Anti-Fraud and Bribery Policy statement on GTCNI's website www.gtcni.org.uk.

Definition of Fraud

The Fraud Act 2006 became law in January 2007 and it applies to England, Wales and Northern Ireland. It replaces the existing complicated array of over specific and overlapping deception offences and establishes a new general offence of Fraud which can be committed in three ways:

- (Section 2) by false *(untrue or misleading, and the person knows this to be the case)* representation;
- (Section 3) by *(dishonestly)* failing to disclose information *(which he/she has a legal duty to disclose)*; and / or
- (Section 4) by abuse of position *(occupies a position in which he/she is expected to safeguard, or not to act against, the financial interests of another person)*.

and in doing so, intends to make a gain for him-/herself or another and to cause loss to another, or expose another to a potential loss. In terms of abuse of position, a person may be regarded as having abused his/her position even though his/her conduct consisted of an omission rather than an act.

The Fraud Act also establishes a number of specific offences to assist in the fight against fraud. These include an offence of possessing articles for use in fraud and an offence of making or supplying articles for use in fraud.

Fraud can be perpetrated by persons outside as well as inside an organisation. The criminal act is the attempt to deceive and attempted fraud is therefore treated as seriously as accomplished fraud.

Computer fraud is where information technology equipment has been used to manipulate programs or data dishonestly (for example, by altering, substituting or destroying records, or creating spurious records), or where the use of an IT system was a material factor in the perpetration of fraud. Theft or fraudulent use of computer time and resources is also included in this definition.

The suspicion that any of these acts has taken place should be regarded as potentially fraudulent and acted upon.

At a basic level four elements are normally necessary for a fraud to occur:

- People to carry out the fraud. They may be individuals within the organisation, outside the organisation, and/or a group of people working inside or outside the organisation;
- Assets of some form to acquire fraudulently;
- Intent to commit the fraud; and
- Opportunity.

For the purposes of this policy, fraud is defined as the use of deception with the intention of gaining an advantage, avoiding an obligation or causing loss to another party. For practical purposes fraud may include such acts as deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts and collusion. The criminal act is the attempt to deceive; attempted fraud is therefore treated as seriously as accomplished fraud.

Managers must ensure that the opportunities for fraud are minimised. Opportunities to commit fraud may be reduced by ensuring that a sound system of internal control, proportional to risk, has been established and that it is functioning as intended. While some people would never contemplate perpetrating a fraud, others may if they thought they could do it without being detected. A high chance of being caught will often deter such individuals.

Definition of Bribery

The Bribery Act 2010, which came into force in 2011, makes it an offence for a UK national or person located in the UK to pay or receive a bribe, either directly or indirectly. It covers transactions that take place in the UK or abroad, and both in the public or private sectors.

A bribe is an inducement or reward offered, promised or provided in order to gain any commercial, contractual, regulatory or personal advantage.

Organisations can also commit an offence for failing to prevent bribery, where a bribe has been paid on their behalf by an "associated person". "Associated persons" include employees, agents and any person performing services for or on behalf of the organisation.

Where an organisation commits an offence, senior officers of that organisation can also be held liable.

There is a defence available to this corporate offence to have "adequate procedures" in place to prevent bribery.

GTCNI's Responsibilities

Accounting Officer Responsibilities

In his role as Accounting Officer, the Interim Chief Executive Officer (CEO)/Registrar is required to sign off the Annual Report and Accounts each year. A key element of the Annual Report and Accounts is the Governance Statement. In signing off the Governance Statement, the Interim CEO/Registrar provides a personal assurance to all of GTCN's customers and stakeholders that there is a system of internal financial and managerial control which is based on a framework of regular management information, financial regulations, administrative procedures and a system of delegation and accountability.

Annex 4.7 of Managing Public Money Northern Ireland (MPMNI) should also be read in conjunction with this policy.

GTCNI, as an ALB within the Department for Education (DE), supports participation in the National Fraud Initiative whereby reports on data matches with other organisations are investigated for the purposes of detecting instances of fraud, over or underpayments and other errors. This is directed by NIAO's Comptroller and Auditor General (C&AG), who has statutory powers to conduct data matching exercises for the purpose of assisting in the prevention and detection of fraud. The powers are contained in Articles 4A to 4H of the Audit and Accountability (Northern Ireland) Order 2003 as inserted by the Serious Crime Act 2007. Bodies, such as GTCNI, who are audited by the C&AG or Local Government Auditor may be required to submit data for matching under the NFI.

GTCNI will also follow NIAO's guidance on Managing the Risk of Bribery and Corruption.

GTCNI's Anti-Fraud and Bribery Policy is intended to demonstrate to all those that seek to defraud the organisation that such action is unacceptable and will not be tolerated.

GTCNI undertakes to ensure that procedures, guidance and approvals regarding Hospitality and Procurement of Goods and Services are appropriately implemented to mitigate against the risk where a person associated with a commercial organisation bribes an employee with the intention of obtaining or retaining business or a business advantage for the commercial organisation, as this could result in a judgement against GTCNI as guilty of an offence under the Bribery Act and liable for an unlimited fine. These policies should also be read in conjunction with this policy.

GTCNI will initiate an investigation where there is suspected fraud and/or bribery and take the appropriate legal and / or disciplinary action in all cases where that would be justified.

Where there is fraud and/or bribery (proven or suspected), GTCNI will make any necessary changes to systems and procedures to prevent similar frauds or opportunities for bribes occurring in the future.

GTCNI has established systems for recording, monitoring and reporting all discovered cases of fraud and/or bribery (proven or suspected).

Although the Interim CEO, as Accounting Officer, bears overall responsibility and is liable to be called to account for specific failures, these responsibilities fall directly on line management and many involve all of GTCNI's staff.

Head of Corporate Services Responsibilities

Overall responsibility for managing the risk of fraud has been delegated to the Head of Corporate Services. Other GTCNI Managers also have a key responsibility to take steps, as are reasonably open to them, to prevent and detect fraud.

Responsibilities of the Head of Corporate Services include:

- Developing GTCNI's Fraud Risk Register and overseeing regular reviews of the corporate fraud risks assessments in order to keep the Register current;
- Establishing an effective anti-fraud policy and fraud response plan, commensurate to the level of fraud risk identified in GTCNI's Fraud Risk Register;
- Designing an effective control environment to prevent fraud commensurate with the level of fraud risk;
- Assessing the risk of the organisation being used for money laundering;
- Advising SMT and Line Managers on the conduct of fraud investigations;
- Liaising where necessary with DE Group Fraud Investigation Services (GFIS), and DE Head of Internal Audit in accordance with the Fraud Response Plan;
- Ensuring that vigorous and prompt investigations are carried out if fraud occurs, is attempted or is suspected and appropriate action is taken to recover assets and losses;
- Establishing appropriate mechanisms for:
    - Reporting fraud risk issues;
    - Reporting significant incidents of fraud to the Accounting Officer;
    - Staff to report all instances of suspected or actual fraud to line management who must then report to the Head of Corporate Services;
    - Reporting, externally, to DoF AFMD and the Comptroller and Auditor General, Northern Ireland Audit Office (NIAO), in accordance with MPMNI Annex 4.7;
    - Coordinating assurances about the effectiveness of the anti-fraud policy and fraud response plan to support the Department's annual Governance Statement;
    - Liaising with GIST and DE Audit and Risk Assurance Committee;

- Making sure that all staff are aware of GTCNI's anti-fraud policy and know what their responsibilities are in relation to combating fraud; and
- Ensuring that appropriate action is taken to minimise the risk of similar frauds occurring in future.

Within Corporate Services, specific HR responsibilities include requirements to ensure that:

- Appropriate pre-employment screening measures are undertaken;
- Anti-fraud awareness training is provided as appropriate and, if necessary, more specific anti-fraud training and development is provided to relevant staff;
- Providing advice and support to management in implementing suspensions and any subsequent disciplinary investigation, including advising on the application of GTCNI's Disciplinary Policy;
- Where appropriate, legal and/or disciplinary action is taken against perpetrators of fraud;
- Where appropriate, disciplinary action is taken against supervisors where supervisory failures have contributed to the commission of fraud, and
- Where appropriate, disciplinary action is taken against staff who fail to report fraud.

Line Managers' Responsibilities

SMT and line managers are 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 therefore rests primarily with SMT as senior line managers.

There is a need for all managers to:

- Take steps to provide reasonable assurance that the activities of GTCNI are conducted honestly and that its assets are safeguarded, including assessing the fraud risk involved in the operations/area for which they are responsible;
- Sign off the business area's fraud risk assessment(s) every 6 months and on each occasion they are amended (if sooner);
- Ensure, that to the best of their knowledge and belief, financial information, whether used in the organisation operations, business or for financial reporting, is reliable;
- Establish arrangements designed to deter fraudulent or other dishonest conducts and ensuring that these arrangements are complied with;
- Where a fraud has taken place, implement new controls to reduce the risk of similar fraud;

- Report any instances of suspected or proven fraud to the Head of Corporate Services as soon as they become aware of such instances;
- Where appropriate oversee the conduct of fraud investigations and liaising where necessary with the Head of Corporate Services in accordance with the Fraud Response Plan;
- Ensure that appropriate action is taken to recover assets and losses; and
- Provide updates on open fraud cases.

Line managers must ensure that opportunities for employees to commit fraud are minimised.

The Head of Corporate Services, supported by DE's Head of Internal Audit is available to offer advice and assistance to line managers as necessary.

As fraud prevention is the ultimate aim, anti-fraud measures should be considered and incorporated in every system and programme at the design stage, e.g. the design of application forms, regular monitoring of expenditure etc. DE Internal Audit is available to offer advice to managers on risk and control issues in respect of existing and developing systems/programmes.

In relation to the personal conduct of employees, line managers should:

- ensure that employees under their control have read and understood the Code of Ethics for Staff of GTCNI;
- ensure that employees under their control have read and understood GTCNI's Conflicts of Interest Policy;
- encourage employees to make internal disclosures of malpractice under the Public Interest Disclosure Order (PIDO);
- ensure that employees under their control are aware of the rules relating to confidentiality of information;
- ensure that employees under their control have been made aware that fraudulent activity is wrong and are aware of the consequences of involvement in fraudulent activity;
- assess the types of risk involved in the business areas for which they are responsible;
- regularly review and test the control systems for which they are responsible;
- ensure that controls are being complied with by all employees;
- satisfy themselves that their systems continue to operate effectively;
- provide assurances on their internal control systems; and
- raise fraud awareness among employees and clients e.g. through awareness seminars, producing fraud reports to highlight instances of fraud etc.
- however, GTCNI acknowledges that, in general, hospitality is seen as an area in which bribery is often involved,

- regularly reinforce the rules relating to personal conduct; and
- employees are aware of the indicators of fraud relating to their business area.
- In addition to identifying risk in their business areas, managers should ensure the register to record gifts and hospitality is appropriately completed and forwarded to Corporate Services. It is more unlikely that hospitality intended to build good business partnership relations would result in a charge of bribery.

Line Supervisors Responsibilities

First Line supervisors / other operational senior officers, responsible for specific teams or functions within a business area (example within Registration, Corporate Services, CEO office) are responsible for ensuring that an adequate system of internal control exists within their areas of responsibility and that controls operate effectively.

Responsibility for the prevention and detection of fraud, therefore, rests primarily with first line supervisors or managers.

A major element of good corporate governance is a sound assessment of the organisation's business risks. With the support of the Head of Corporate Services, first line Supervisors / Managers need to ensure that:

- Fraud risks in their business areas have been identified for inclusion within GTCNI's risk registers based on a review of the operations/area for which they are responsible;
- Each risk has been assessed for likelihood and potential impact;
- Adequate and effective controls have been identified for each risk;
- Controls are being complied with, through regular review and testing of control systems;
- Risks are reassessed as result of the introduction of new systems or amendments to existing systems;
- Where a fraud has occurred, or has been attempted, controls are reviewed and new controls implemented, as necessary, to reduce the risk of fraud recurring; and
- Fraud occurrences are quantified on an annual basis and Risk Registers updated to reflect the quantum of fraud within the Business Area. Where appropriate, strategies should be devised to combat recurrence of fraud and targets set to reduce the level of fraud.

In terms of establishing and maintaining effective controls, it is desirable that:

- Where possible, there is a regular rotation of staff, particularly in key posts;
- Wherever possible, there is a separation of duties so that control of a key function is not vested in one individual;
- Backlogs are not allowed to accumulate, and
- In designing any new system, consideration is given to building in safeguards to prevent and/or detect internal and external fraud.

In relation to the personal conduct of employees, first line supervisors / managers should:

- ensure that employees under their control have read and understood the Code of Ethics for Staff of GTCNI;
- ensure that employees under their control have read and understood GTCNI's Conflicts of Interest Policy;
- encourage employees to make internal disclosures of malpractice under the Public Interest Disclosure Order (PIDO);
- ensure that employees under their control are aware of the rules relating to confidentiality of information;
- ensure that employees under their control have been made aware that fraudulent activity is wrong and are aware of the consequences of involvement in fraudulent activity;
- regularly review and test the control systems for which they are responsible;
- ensure that controls are being complied with by all employees;
- satisfy themselves that their systems continue to operate effectively;
- regularly reinforce the rules relating to personal conduct; and
- ensure Hospitality Registers are appropriately completed.

Employees' Responsibilities

As effectively stewards of public funds (teacher registration fee income), GTCNI employees must act with, and be seen to have, the highest standards of personal integrity.

Policies on Gifts and Hospitality and guidance on Procurement of Goods and Services should also be read.

Every member of staff has a duty to ensure that members' funds are safeguarded and therefore, everyone is responsible for:

- Acting with propriety in the use of official resources and the handling and use of funds in all instances. This includes cash and/or payment systems, receipts and dealing with suppliers;
- 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
- Being vigilant to the possibility that unusual events or transactions could be indicators of fraud and alerting their line supervisor or manager where they believe the opportunity for fraud exists. Appendix 1 provides examples of Indicators of Fraud. In addition, Risks and Controls in Specific Systems are

included in Appendix 2, with guidance on Reducing Opportunities for Fraud detailed in Appendix 3.

In addition, it is the responsibility of every member of staff to report details immediately to their line supervisor / manager or the Head of Corporate Services if they suspect that a fraud has been attempted or committed, or see any suspicious acts or events. More details on reporting are included in GTCNI's Fraud Response Plan.

The Public Interest Disclosure (NI) Order 1998 Guidance on Public Interest Disclosure (Raising Concerns - 'whistleblowing') – protects the rights of staff who report wrongdoing. If you are in any doubt, you should speak to a senior officer. A GTCNI Whistleblowing (Raising Concerns) Policy has been developed and can be found on GTCNI's M: Drive in Staff Resources and information is also available in Appendix 4.

Advice is also available through the independent charity Protect.

Section 5 of the Criminal Law Act (Northern Ireland) 1967 (Withholding Information) also places the onus on individuals to report/pass evidence 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 members' funds, all staff in GTCNI must have, and be seen to have, high standards of personal integrity. Staff including temporary staff or contractors should not accept gifts, hospitality or benefits from a third party, which might be seen to compromise their integrity. GTCNI has specific guidance on The Provision and Acceptance of Gifts and Hospitality, and this guidance also applies to gifts or hospitality offered to spouses, partners or other associates of a member of staff if it could be perceived that the gift or hospitality is in fact for the benefit of that member of staff.

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.

Every employee has a duty to ensure that public funds are safeguarded, whether they are involved with cash or payments systems, receipts, inventories or stocks or dealings with contractors or suppliers or with registered teachers or applicants.

Employees should not place themselves under any financial or other obligation to outside individuals or organisations who might influence them in the performance of their official duties by way of blackmail, fraud or bribe.

Employees should always be aware of the need not to give the impression to any member of the public or organisation with whom they deal, or to their colleagues, that they may be influenced, or have previously or already been influenced, by any gift or

consideration to show favour to any person or organisation whilst acting in an official capacity on behalf of GTCNI.

Employees should alert their line manager where they believe the opportunity for fraud exists because of poor procedures, lack of effective oversight or lack of separation of duties giving rise to a situation where one person has complete control over a process.

Employees should inform line management of any outside interest which might impinge on their discharge of duties or potentially create a conflict of interest.

Employees should ensure that any procurement of Goods and Services does not take place without all of GTCNI's financial and procurement procedures being adhered to, including business case approvals, purchase order numbers and line manager approvals and sign-off, among others.

The UK Bribery Act 2010 essentially creates two general offences of:

- bribing another person (active bribery) (Section 1 of the Act); and
- being bribed (passive bribery) (Section 2 of the Act).

It also creates a discrete offence of bribery of a foreign public official (Section 6) and a new offence of failure of commercial organisations to prevent bribery by persons associated with them (Section 7).

If anyone offers you a bribe on a work related matter or if you are aware of others being bribed, you should report this to your supervisor or line manager.

GTCNI's Whistleblowing and Raising Concerns at Work Policy gives guidance to employees on procedures to be observed if they wish to make disclosures of information relating to malpractice by their employer or colleagues at work.

Internal Audit Service Provider's Responsibilities

GTCNI's internal auditors are currently DE Internal Audit.

Internal Audit is responsible for:

- providing an opinion to the Interim Chief Executive on the adequacy of arrangements for managing the risk of fraud and ensuring that GTCNI promotes an anti-fraud culture:
- assisting in the deterrence and prevention of fraud by examining and evaluating the effectiveness of controls applied throughout GTCNI business areas and ensuring that management has reviewed its risk exposure and identified the possibility of fraud as a business risk; and
- assisting GTCNI SMT in conducting fraud investigations.

Fraud Investigation

Line supervisors / line managers should be alert to the possibility that unusual events or transactions can 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 GTCNI policy that there will be consistent handling of all suspected fraud cases without regard to position held or length of service, and investigators should have free access to all staff, records and premises in order to carry out investigations.

After suspicion has been roused, prompt action is essential, and all cases of suspected or actual fraud should be reported immediately to the Head of Corporate Services who can provide advice on next steps.

Line supervisors / managers should not undertake preliminary enquiries until any suspicion has been reported to and advice taken from the Head of Corporate Services.

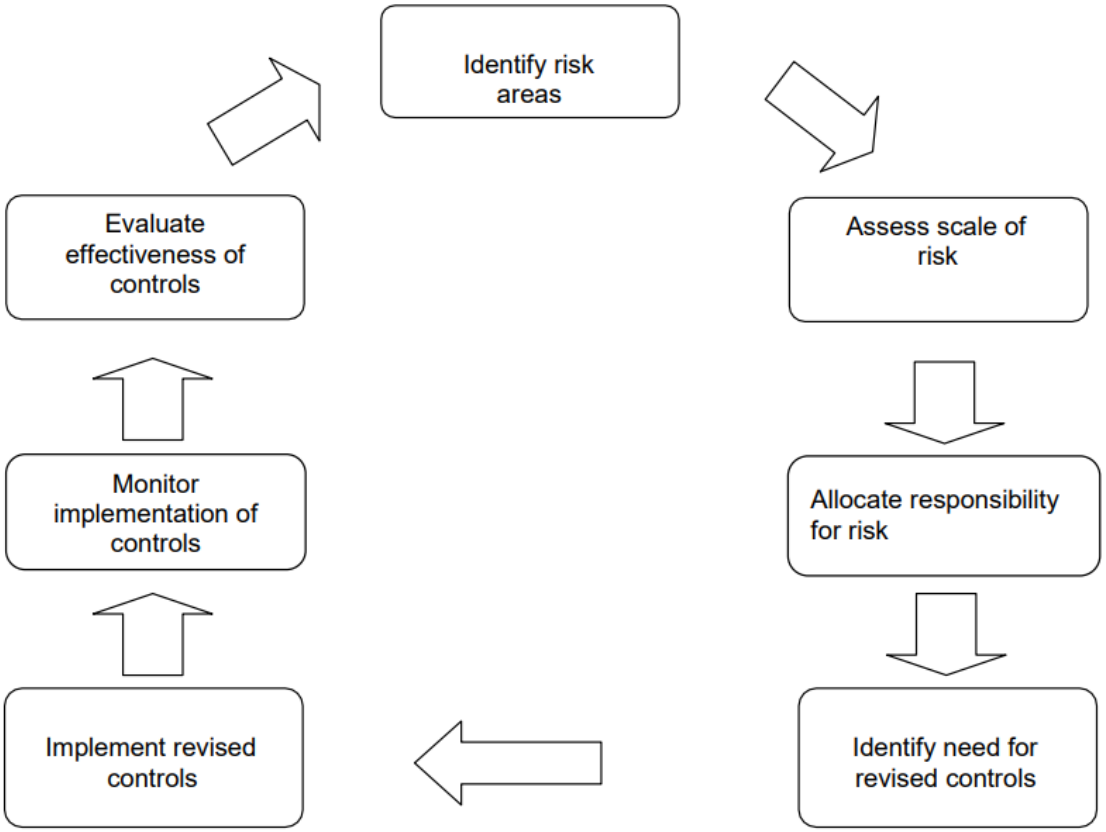
As detailed in the Fraud Response Plan, it is imperative that enquiries should not prejudice subsequent investigations or corrupt evidence, therefore if an initial examination confirms the suspicion that a fraud has been perpetrated or attempted, management should follow the procedures provided in GTCNI's Fraud Response Plan.

Fraud Risk Assessment

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 departments will be exposed.

Figure 1 below sets out the key stages of a risk management cycle to help deal with fraud. Corporate Services, supported by DE Internal Audit, is available to offer advice and assistance on risk management/ internal control issues. In addition Appendix 5 provides Guidance on Performing an Assessment of Fraud Risks.

Figure 1: Risk Assessment Cycle



Disciplinary Action

After full investigation GTCNI will take legal and/or disciplinary action in all cases where it is considered appropriate. Any member of staff found guilty of a criminal act will be considered to have committed a serious disciplinary offence and will be dismissed from the organisation on the grounds of gross misconduct.

Where supervisory negligence is found to be a contributory factor, disciplinary action may also be initiated against those managers/supervisors responsible.

It is GTCNI policy that, where appropriate, all cases of fraud, whether perpetrated or attempted by a member of staff or by external organisations or persons, will be referred to the PSNI at the earliest possible juncture.

Appropriate steps will be taken to recover all losses resulting from fraud, 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. GTCNI takes fraud very seriously, taking a zero tolerance approach, 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, including recovery of losses. Managers should be fully aware of their responsibility to protect members' funds and as such, should always be alert to the potential for fraud.

Fraud Response Plan

Fraud Response Initiation

Staff are often the first to realise that there is something seriously wrong. However, they may not express their concerns because they feel that speaking up would be disloyal to their colleagues or the organisation, or because they fear harassment or victimisation.

GTCNI's Whistleblowing and Raising Concerns Policy is intended to encourage and enable both staff and members of the public to raise serious problems within the organisation rather than overlooking them or going directly to the media or an external organisation. Staff and members of the public should follow the guidance in the whistleblowing and raising concerns policy. Requests for confidentiality will be respected as far as possible. However, to gain the protection given to whistle-blowers under the Public Interest Disclosure Act 1998 (PIDA) and Amendment Order 2022, the person (s) must disclose their identity.

A designated member of staff will act as a contact point for staff and the public if they wish to discuss suspicions of fraud or bribery. GTCNI has appointed the Head of Corporate Services as the designated senior manager, with escalation to the Interim CEO, if necessary, to undertake this role. Members of the public who suspect fraud or bribery should be encouraged to contact the designated person either in writing, by telephone or by making an appointment to meet them. Members of the public are not covered by the legal remedies noted in the Public Interest Disclosure Act 1998 / updated Amendment Order (NI) 2022, as there is no employment relationship with the public sector organisation.

If a manager receives information from a member of staff, they should:

- deal with the member(s) of staff giving the information in a way that shows that their concerns are being taken seriously;
- ensure that they do not belittle or dismiss the information;
- emphasise what the member(s) of staff should not do (see below);
- respect, as far as possible, the confidentiality of the member(s) of staff;

- attempt to identify where any evidence may be, but not attempt to obtain it or to question anybody;
- follow the approved procedure for passing on the information.

If a member of staff suspects fraud or bribery, it is important that they:

- do not approach the person, people or organisation suspected, but tell only the member of staff named in the fraud/bribery response plan;
- do not attempt to collect evidence or question anybody. If they have documents etc. which they think are relevant, they should secure them safely;
- make a note of the time, date and the details of anything they see or hear that they think is relevant;
- do not attempt to investigate alone; and
- seek advice, in confidence, from internal or external audit or an appropriate manager if they are unsure about what has been seen or heard.

Fraud Investigations

The Interim CEO and Head of Corporate Services will be responsible for investigations.

Investigative procedures as outlined within the Fraud Response Plan and Whistleblowing and Raising Concerns Policy will be followed.

The gathering of evidence and interviewing of witnesses or suspects must all be carried out to standards that satisfy legislation, including the Human Rights Act (1998), the Police and Criminal Evidence Act (1984) and the Regulation of Investigatory Powers Act (2000). This standard of operating applies equally to any type of investigation whether the outcome is likely to be criminal prosecution, civil recovery or internal disciplinary action.

GTCNI also has an audit function (internal and external) that can provide an independent opinion on the effectiveness of financial systems, financial reporting and an assessment of risks.

Any member of staff who wishes to raise concerns under this policy should first speak to their line manager or put the concern in writing to their line manager. If it is not appropriate - for any reason - to report to the line manager, the member of staff may speak directly to the Interim CEO or Head of Corporate Services. If the member of staff does not wish to be identified, they should say this at the first possible opportunity so that appropriate arrangements can be made.

The line manager will note the key points of the concern and check that the member of staff has a copy of the whistleblowing and raising concerns policy.

The line manager will then refer the concern to the Interim CEO or Head of Corporate Services, who has responsibility for concerns raised under this policy, and hand over any written materials.

The action taken by the designated senior manager will depend on the nature of the concern. The manager will try to establish at an early stage whether it appears that a criminal act has taken place, as this will shape the likely course of further action.

Within [10] working days, the designated senior manager will write to the complainant acknowledging the complaint and indicating how they intend to deal with it. The letter will also give an estimate of how long it will take to provide a final response.

If it appears that a criminal act has not taken place, an internal investigation will be undertaken to determine the facts and consider what action, if any, should be taken against those involved.

Any action taken against a member of staff will follow GTCNI's disciplinary procedure but, in addition, the organisation may seek to recover any loss incurred through civil proceedings. The investigation will also look at how internal controls could be improved to prevent the problem from happening again.

If it appears that a criminal act has taken place, the designated senior manager will contact the police.

The designated senior manager will keep full records of the complaint and all actions taken to investigate it.

GTCNI recognises that people who have reported instances of fraud or corruption need to be assured that the matter has been properly addressed. Subject to any legal constraints, the designated senior manager will provide information about the outcomes of any investigation to the complainant at the conclusion of the investigation.

Sanctions for Breach

A breach of any of the provisions of this policy will constitute a disciplinary offence and will be dealt with in accordance with the appropriate disciplinary procedure. Depending on the gravity of the offence, it may be treated as gross misconduct and could render the employee liable to summary dismissal.

As far as associated persons are concerned, a breach of this policy could lead to the suspension or termination of any relevant contract, sub-contract or other agreement.

Legal Remedy - Public Interest Disclosure (NI) Order 1998 / Public Interest Disclosure (Prescribed Persons) (Amendment) Order (NI) 2022

Workers have a retrospective remedy in employment law, in that they can take a case against their employer at an employment tribunal if they are victimised or suffer detriment as a result of raising a concern.

This legal remedy is not available to a member of the public raising a concern, as there is no employment relationship with the public sector organisation.

The Public Interest Disclosure (NI) Order 1998, as amended by the 2014 Amendment Order, subsequently revoked by the 2022 Amendment Order, provides recourse to an employment tribunal if you suffer detriment, such as dismissal or other sanction, as a result of raising concerns which you believe to be true. Your case at tribunal is strengthened if you raise your concerns with your employer in the first instance. Your employer's policy for raising concerns should tell you how you can do this safely. The Public Interest Disclosure Order will also apply if you raise your concerns externally to the relevant "prescribed person". If you do so anonymously, protection under PIDA will not apply.

The following links will take you to the legislation:

- Public Interest Disclosure (NI) Order 1998
- Public Interest Disclosure (Prescribed Persons) (Amendment) Order (Northern Ireland) 2022.

Other External Resources in Identifying and Managing Fraud

The Comptroller and Auditor General (C&AG) at the NI Audit Office (NIAO) has published a range of guidance in identifying and managing different types of fraud risk and this guidance has been embedded in GTCNI's policy. Helpful links include:

- Managing Fraud Risk in a Changing Environment
- Managing the Risk of Bribery and Corruption
- Covid-19 Fraud Risks NIAO August 2020
- Procurement Fraud Risk Guide
- Grant Fraud Risks
- Internal Fraud Risks

Helpful Contacts

Department of Education
Rathgael House, Balloo Road, Rathgill, Bangor BT19 7PR
Contact: Carolyn Shaw, Head of Internal Audit
Tel: 028 9127 9977 Email: carolyn.shaw@education-ni.gov.uk

Northern Ireland Audit Office
106 University Street, Belfast BT7 1EU
Tel: 028 9025 1000 Email: raisingconcerns@niauditoffice.gov.uk

Equality Commission for Northern Ireland
Equality House, 7-9 Shaftesbury Square, Belfast BT2 7DP
Tel: 028 9050 0600 Email: information@equalityni.org

Police Service of Northern Ireland
Tel: 101 Web: https://www.psni.police.uk/contact-us/

Alternatively, free confidential advice can be obtained from Protect, the UK's whistleblowing charity, by ringing 020 3117 2520. As a legal advice service, Protect offers free expert and confidential advice on how best to raise your concern and your protection as a whistleblower. If you are unsure or unaware of how to raise a concern, contact Protect. For more information, visit their website at Protect - Speak up stop harm (protect-advice.org.uk).

Policy Review

This policy will be reviewed every 3 years.

Policy Compliance

All staff are required to confirm that they have read and understood this policy and its application within GTCNI. Please confirm by emailing the following to mary.jackson@gtcni.org.uk

I **[insert full name]** confirm that I have read, understood and will adhere to GTCNI's Anti- Fraud and Bribery Policy.

APPENDICES

Appendix 1 - Indicators of Fraud

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.
- 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.

Appendix 2 - Examples of Risks and Controls in Specific Systems

Cash Handling

There are many risks associated with cash handling. Theft or misappropriation of cash may be assisted by the suppression, falsification or destruction of accounting records, or where no initial records are created at all. This section suggests some controls that should be in place.

How fraud could be perpetrated	Examples of controls
Theft	• Hold cash securely at all times. • Restrict access to cash to named personnel. • Hold keys securely and limit access to authorised personnel. Keep cash balances to a minimum. • Maintain transaction records. • Carry out periodic and independent checks and reconciliations.
Income received not brought to account	• Issue pre-numbered receipts (ideally receipts should be generated automatically). Maintain prompt and accurate records of income received. • Ensure post-opening duties are carried out by at least two people and receipts log completed and signed by both officers. • Separate duties at key stages of the process: - bringing receipts to account and preparation of cash and cheques for banking - daily cash balancing and bank reconciliations. • Establish regular and random management checks of source documentation, accounting records and bank reconciliations. • Rotate staff duties frequently.
Illegal transfer or diversion of money. Changes and additions to payee details through BACS.	• Ensure that changes and additions to payee details and other standing data are properly authorised. • Restrict and log system access to make and authorise these changes. • Provide adequate supervision of all staff particularly new, inexperienced or temporary staff. • Ensure payments are authorised before they are made. • Restrict knowledge of transfer codes (and passwords if payments are initiated internally by computer) to approved personnel. • Change transfer codes and passwords frequently and always when staff leave. Passwords and User Ids should always be suspended when a member of staff leaves. Ensure that payment reports are independently reviewed for accuracy immediately before the transfer of funds occurs. • Separate duties (e.g. between those setting up payment accounts and those authorised • to trigger payments and between those receiving goods and services and those who process and make payments).

Accounting records are falsified or amended to allow unauthorised payments	• Ensure that amendments and deletions to accounting records are authorised. Carry out independent checks to ensure amendments have been made correctly. Establish authorisation levels. • Perform frequent independent checks, including spot checks. • Reconcile accounting records and petty cash frequently, maintain reconciliation records and carry out independent reviews, investigate and resolve all discrepancies. • Report any discrepancies that cannot be resolved, or any losses that have occurred. Regularly review suspense accounts to confirm their validity.
Invoices are falsified or duplicated in order to generate false payment.	• Segregate duties between ordering and payment of invoices. Carry out routine checks: • - Invoice has a genuine purchase order number. • - Match invoice to purchase order and goods received note. • - Check invoice detail looks right, that amounts and calculations are correct etc. • - Ensure invoice had not already been paid, by checking relevant records.
Supplier bank account details are changed in order to divert payments.	• Only accept requests for changes to supplier standing data in writing. • Seek confirmation from the supplier that the requested changes are genuine using contact details held on the vendor data file or from previous and legitimate correspondence. Do not contact the supplier via contact details provided on the letter requesting the changes. • Ensure that there is segregation of duties between those who authorise changes and those who make them. • Maintain a suitable audit trail to ensure that a history of all transactions and changes are maintained. • Produce reports of all changes made to supplier standing data and check that the changes were valid and properly authorised before any payments were made. • Regularly verify the correctness of standing data with suppliers.
Unauthorised use of cheques and payable orders	• Hold financial stationery securely and maintain records of stock holdings, withdrawals and destruction of wasted stationery. • Establish signatories and delegated powers for cheques and payable orders. • Reconcile cheques and payable orders to source documentation before issue. • Use restrictive crossings such as “non-transferable” and “a/c payee”. • Ensure that addresses to which payable instruments are sent are correct. For large value payments check encashment to ensure that the intended recipient did receive the payment. • Discover the fraudulent amendment of cheque details by careful choice of inks and printers so that the print produced on cheques is as indelible as possible. • Print the amount in figures as close to the £ as possible. • Write payee details in full rather than use abbreviations or acronyms. • Fill up blank spaces with insignificant characters such as asterisks. • Use envelopes that make it less obvious that they contain cheques for mailing purposes. • Ensure that signed cheques are not returned to payment staff. • Reconcile bank statements with check listings regularly. Check that there are no missing/out of sequence cheque numbers

Payroll/Travel & Subsistence

Risks that may be associated with the payroll function include the introduction of non-existent (ghost) employees, unauthorised amendments made to input data, and the payment of excessive overtime, bonus or travel claims. This section suggests some controls that should be in place.

How fraud could be perpetrated	Examples of controls
Creating fictitious employees whose pay is then obtained by the fraudster or by someone in collusion, or obtaining pay that is not consistent with the employee's grade.	• Ensure that only authorised personnel are able to update payroll records. • Segregate duties between those responsible for authorizing appointments and those who make changes to standing data and action payments. • Produce listings of all starters, leavers and changes to standing data as part of every payroll run and check that all changes have been made correctly. • Produce regularly exception reports (eg emergency tax codes for more than 6 months, no NI numbers, duplicate payees), for investigation by management. • Subject the payroll master file to periodic checks by HR to ensure that each post is authorised, that the correct person is in post, that the person exists and that basic salaries and allowances are correct. • Provide budget holders with sufficient and timely information to enable them to reconcile staffing costs against budget.
Making false claims for allowances, travel and subsistence	• Establish a comprehensive set of rules and ensure that they are communicated to staff. Establish a formal process that involves line managers approving and reviewing work plans and programmes for visits, especially for staff where there is no countersigning requirement. • Institute checks by countersigning officers of claims against approved work plans, standard mileages for regular destinations and primary evidence such as hotel bills, rail tickets and taxi receipts. • Instruct finance teams to ensure that correct rates are claimed; substantiating documents (eg hotel invoices) are included and check that authorised claims were received from approved countersigning officers. • Establish random sample management checks to verify details on claims and to ensure that finance team checks were applied rigorously to claims. • Provide budget holders with sufficient information to enable them to monitor costs against budget.
Misuse of Corporate Credit Cards	• Establish clear policy/rules and communicate to all staff. • Make one person or central group responsible for issuing cards (e.g. payments section). Authorise all card issues. • Maintain a record of cardholders. Establish monthly credit limits. • Require cardholders to submit expense claims regularly supported by invoices/receipts to the group that process payments for checking and reconciliation to card issuer statements. • Ensure that cards are returned and destroyed when staff move or cease to be cardholders.

Contracting

The section sets out some examples of controls which should be in place, in addition to those which apply generally to cash handling and purchasing systems, to counter the fraud risks faced in relation to the use of contractors.

How fraud could be perpetrated	Examples of controls
A contractor could be selected as a result of favouritism or who does not offer best value for money	• Draw up and agree a clear and comprehensive specification. • Use a Central of Procurement Expertise to carry out the tendering and letting procedures. Comply with Procurement Guidance Notes. • Seek tenders from suitable suppliers (must comply with EC/GATT regulations). Draw up clear and comprehensive tender evaluation criteria. • Arrange for tenders to be delivered to those responsible for selection without interference. Do not accept late tenders. • Ensure that tenders are evaluated against the agreed evaluation criteria by a tender evaluation board. • The Project Board should approve the successful contractor. • Require staff to declare any personal interests they may have which may affect the tendering process.
Payments made for work not carried out as a result of collusion between contractor and official	• Ensure that invoices are supported by independent certification that work was performed satisfactorily before authorising payment. • Maintain a register of contracts in progress. • Only add approved and authorised contracts to the register. Accept invoices from approved contractors only. • Ensure that all contract variations are supported by sequentially numbered and • authorised variation orders before payment.

Purchasing

Risks associated with the operation of purchasing systems include the false input of invoices, the diversion of payments and misappropriation of purchases. This section sets out some examples of controls that should be in place to reduce the risk of fraud in this area.

How fraud could be perpetrated	Examples of controls
Unauthorised use of purchasing systems in order to misappropriate goods or use services for personal gain.	• Restrict opportunity to generate payment by using sequentially numbered purchase order forms for all orders; perform independent checks to show that purchase orders are valid and accounted for. • Establish authorised signatories and authorisation limits for requisitioning and placing orders. • Match invoices with orders before the invoice is certified for payment. • Keep stock records up to date so that stocks, stock usage and orders can be monitored. • Separate the duties between those ordering, receiving goods, and approving and paying invoices. This separation of duties should be reviewed regularly. • Ensure that authorised staff make amendments to standing data (e.g. supplier records). • Provide budget holders with sufficient and timely information to enable them to reconcile expenditure against budget.
Short deliveries of goods or services	• Check delivery notes to original orders, chase up short deliveries, and only pay for goods received.
Acceptance of unsolicited goods or expanded orders as a result of fraudulent acceptance of attractions such as free gifts.	• Confirm goods were properly ordered, authorised and received before authorising payment. • Only pay for goods ordered.
Misuse of Government Procurement Cards (GPC)	• Establish a clear GPC policy that is communicated to all staff and should include expenditure limits for individual transactions. • Appoint an individual to be the cardholder manager who will be responsible for appointing cardholders and for dealing with the card issuing bank. • Maintain a list of authorised cardholders. • Cardholders should maintain a log of all transactions that should be supported by authorisations to make purchases, invoices/receipts. • Cardholders must hold cards securely. • Cardholders must check all entries on statements supplied by the bank and refer any discrepancies to the cardholder manager. • Budget holders should carry out periodic checks to ensure that GPC statements are properly reconciled and that only authorised purchases are made. • Ensure that cards are returned to the cardholder manager and
	cancelled with the bank when cardholders move or cease to be cardholders. The cardholder manager should also ensure that the card is destroyed and the record of cardholders amended.
Orders placed on the Internet are not delivered or goods received are not of the desired quality	• Make sure your browser is set to the highest level of security notification and monitoring. • Check that you are using the most up to date version of your browser and ensure their security features are activated. • Keep a record of the retailer's contact details, including a street address and non-mobile telephone number. Beware if these details are not available on the website. Do not rely on the e-mail address alone. • Click on the security icon to see if the retailer has an encryption certificate. This should explain the type and extent of security and encryption it uses. Only use companies that have an encryption certificate and use secure transaction technology. • If you have any queries or concerns, telephone the company before giving them your card details to reassure yourself that the company is legitimate. • Print out your order and consider keeping copies of the retailer's terms and conditions and returns policy. Be aware that there may well be additional charges such as postage and VAT, particularly if you are purchasing goods from traders abroad. When buying from overseas always err on the side of caution and remember that it may be difficult to seek redress if a problem arises. • Check statements from your bank or card issuer carefully as soon as you receive them. Raise any discrepancies with the retailer concerned in the first instance. If you find any transaction on your statement that you are certain you did not make, contact your card issuer immediately. • Check that you are fully aware of any payment commitments you are entering into, including whether you are instructing a single payment or a series of payments. • Never disclose your card's PIN to anyone, including people claiming to be from your bank or the Police, and NEVER write it down or send it over the internet. • If you have any doubts about giving your card details, find another method of payment.

Assets

Risks in this area include use of assets for personal gain, or misappropriation of assets. This section suggests some controls that should be in place to counter those risks.

How fraud could be perpetrated	Examples of controls
Theft or unauthorised use of assets	• Maintain up to date asset registers and inventories • Ensure that assets are assigned to individual budget centres. • Clearly describe assets in registers and inventories. • Mark assets in some way (e.g. property of xxx). • Store assets securely. • Carry out regular spot checks to confirm existence of assets.

Information

This section deals with some of the controls that should be in place to reduce the threat of fraud or other irregularities arising from access to sensitive information or misuse of information for private gain.

How fraud could be perpetrated	Examples of controls
Theft of sensitive/restricted documentation or information	• Identify all information assets. • Produce a clear information risk policy and communicate to all staff. • Implement the Government Mandatory Minimum Measures for managing information risk. • Define key roles and responsibilities for managing information risk (e.g. Senior Information Risk Owner, Information Asset Owners) and allocate to named individuals. • Establish an effective information risk governance framework. • Ensure that data security arrangements are underpinned by a culture that values and protects data. • Carry out regular assessments of the information risks and whenever changes occur to technology or new threats are identified. • Restrict access to information on a need to know basis. • Ensure that access rights are reviewed regularly and that these are removed for staff that leave. • Limit the use of removable media (eg laptops, USB memory sticks, CDs). Encrypt data transferred to removable media. • Do not use e-mail to transmit confidential information unless it is encrypted. • Regularly check the activities of those with rights to transfer personal or sensitive data to ensure that they continue to have a business case for these activities. • Ensure that all data users successfully undergo information-risk awareness training. • Ensure that contingency arrangements (so that damaged or lost data can be renewed or replenished quickly) are regularly tested. • Put in place arrangements to log activities of data users and for managers to review usage. Computer logs should be adequately protected against unauthorised access and amendment.

Money laundering

While most public bodies are not regulated under the Money Laundering Regulations, bodies could be at risk from criminals using the organisation's systems to launder cash gained through involvement in criminal activities.

How fraud could be perpetrated	Examples of controls
Individuals or groups pass money transactions through organisational systems	• Carry out assessment of the risk the organisation is at from being used to launder “dirty cash”. • Depending on the outcome of such an assessment controls can include: • Developing anti money laundering policies and processes. • Appoint a Money Laundering Reporting Officer. • Provide awareness training to staff. • The Joint Money Laundering Steering Guidance approved by HMT may be a useful source of information in this area.

Appendix 3 - Reducing Opportunities for Fraud

Introduction

The absence of proper control and the failure to observe existing control procedures are the main contributory factors in most frauds. Managers must ensure that the opportunities for fraud are minimised. Separation of duties, effective procedures and checks should prevent or deter fraud from occurring.

Opportunities to commit fraud may be reduced:

- by ensuring that a sound system of internal control proportional to risk has been established and that it is functioning as intended;
- through the “fear factor” (i.e. the risk of being caught or the severity of the consequences);
- by changing attitudes to fraud, and
- by making it too much effort to commit.

Internal Control

“Control” is any action, procedure or operation undertaken by management to increase the likelihood that activities and procedures achieve their objectives. Control is a response to risk – it is intended to contain uncertainty of outcome. Some frauds arise because of a system weakness such as a lack of proper control over e.g. placing of purchase orders. Other frauds are the result of failures to follow proper control procedures. It may be the result of carelessness in carrying out a check, or it may be that too much trust has been placed in one individual with no effective separation of duties. Frauds that result from collusion may be more difficult to detect and prevent as these types of fraud tend to operate within the normal control environment.

In designing control, it is important that the control put in place is proportional to the risk. In most cases it is normally sufficient to design control to give a reasonable assurance of confining loss within the risk appetite of the organisation. Every control action has an associated cost and it is important that the control action offers value for money in relation to the risk that it is controlling. Generally speaking the purpose of control is to contain risk to a reasonable level rather than to remove it entirely.

When risks and deficiencies in the level of control are identified it is necessary to choose the most appropriate type of controls within the above guidelines. In respect of fraud risks prevention is almost always preferable to detection. Strong preventive controls should therefore be applied wherever possible.

The following range of controls should be considered always ensuring that a balance between identified risk and value for money is maintained:

Physical security: this is a preventive measure which controls or monitors access to assets, documentation or IT systems to ensure that there is no unauthorised use, loss or damage.

Assets can range from the computer terminal that sits on the desk to the cheques sent out to pay suppliers. As a general principle all assets should be held securely and access to them restricted as appropriate. The control should apply not only to the premises but also to computers, databases, banking facilities, documents and any other area that is critical to the operation of the individual organisation. It may even be appropriate to restrict knowledge of the existence of some assets.

Access to computer systems is an important area that should be very tightly controlled, not only to prevent unauthorised access and use, but also to protect the integrity of the data - the Data Protection Act requires computer and data owners to secure information held on their systems which concerns third parties. Laptops and computers are also vulnerable to theft, both in terms of hardware and software. This type of theft also has the potential to cause major disruption, significant financial loss or even serious reputational damage to the core operations of an organisation.

Organising: organising involves the allocation of responsibility to individuals or groups so that they work together to achieve objectives in the most efficient manner.

Major principles in organising relevant to fraud are:

- clear definition of the responsibilities of individuals for resources, activities, objectives and targets. This includes defining levels of authority. This is a preventive measure which sets a limit on the amounts which may be authorised by individual officers. To be effective, checks need to be made to ensure that transactions have been properly authorised;
- establishing clear reporting lines and the most effective spans of command to allow adequate supervision;
- separating duties to avoid conflicts of interest or opportunities for abuse. This is also largely a preventive measure which ensures that the key functions and controls over a process are not all carried out by the same member of staff (e.g. ordering goods should be kept separate from receipt of goods); similarly authorisation and payment of invoices; and
- avoiding undue reliance on any one individual.

Supervision and checking of outputs: supervision is the function by which managers scrutinise the work and performance of their staff. It provides a check that staff are performing to meet standards and in accordance with instructions. It includes checks over the operation of controls by staff at lower levels. These act as both preventive and detective measures and involve monitoring the working methods and outputs of staff. These controls are vital where staff are dealing with cash or accounting records. Random spot checks by managers can be an effective anti-fraud measure.

Audit trail: this is largely a detective control, although its presence may have a deterrent effect and thus prevent a fraud. An audit trail enables all transactions to be traced through

a system from start to finish. In addition to allowing detection of fraud it enables the controls to be reviewed.

Monitoring: management information should include measures and indicators of performance in respect of efficiency, effectiveness, economy and quality of service. Effective monitoring, including random checks, should deter and detect some types of fraudulent activity.

Evaluation: policies and activities should be evaluated periodically for economy, efficiency and effectiveness. The management of the operation may perform evaluations, but they are usually more effective when performed by an independent team. Such evaluations may reveal fraud.

Staffing: adequate staffing is essential for a system to function effectively. Weaknesses in staffing can negate the effect of other controls. Posts involving control of particularly high value assets or resources may need the application of additional vetting procedures. Rotation of staff between posts can help prevent or detect collusion or fraud.

Asset accounting: asset registers used for management accounting purposes can help detect losses that may be caused by fraud.

Budgetary and other financial controls: use of budgets and delegated limits for some categories of expenditure and other accounting controls should ensure that expenditure is properly approved and accounted for by the responsible manager. This should limit the scope for fraud and may result in some types of fraud being detected.

Systems development: controls over the development of new systems and modifications to existing systems or procedures are essential to ensure that the effect of change is properly assessed at an early stage and before implementation. Fraud risks should be identified as part of this process and the necessary improvements in control introduced.

These are only some examples of the types of control that can be used to prevent or detect fraud. For examples of internal controls in specific areas see Appendix 2.

The "Fear Factor"

Major deterrents to perpetrating fraud are the risk of being caught and the severity of the consequences. The most important fact about deterrence is that it derives from perceived risk and not actual risk.

GTCNI may manage to increase the actual risk of detection but it will only achieve a deterrent effect if it ensures that perceptions of risk change too.

Ways in which GTCNI can do this include:

- Warnings on forms such as: "false statements may lead to prosecution";
- General publicity;
- Increasing the severity of penalties; and
- Always taking appropriate action against known perpetrators of fraud.

Changing Attitudes to Fraud

The most effective strategies designed to change attitudes rely on motivation rather than fear. They aim to persuade people of the undesirability of a particular behaviour.

Attitude changing strategies rely to a large extent on publicity campaigns to achieve their effect so it is important that GTCNI carry out a full appraisal of the benefits of any proposed advertising campaign and to establish some way of measuring the outcomes of such campaigns. GTCNI need to be clear about the objectives and targets of their campaigns.

Appendix 4 – GTCNI Whistleblowing (Raising Concerns) Operational Arrangements

All of us at some point may have concerns about what is happening at work. However, when it is about unlawful conduct, a possible fraud or a danger to the public or the environment, or other serious malpractice, it can be difficult to know what to do.

You may have worried about raising such a concern and may have thought it best to keep it to yourself, perhaps feeling it was only a suspicion. You may have felt that raising the matter would be disloyal to colleagues, managers or to GTCNI.

You may have decided to say something but found that you have spoken to the wrong person or raised the issue in the wrong way and were not sure what to do next.

GTCNI has put in place Whistleblowing (Raising Concerns) arrangements to reassure you that it is safe and acceptable to speak up. They also enable you to raise any concern about malpractice at an early stage and in the right way. If something is troubling you which you think we should know about or look into, these arrangements set out the steps you should take and identify the key contacts, and our assurances to you. We are committed to making raising a concern work. If you raise a genuine concern under these arrangements, you will not be at risk of losing your job or suffering any form of retribution as a result. Provided you are acting in good faith, it does not matter if you are mistaken. While we cannot guarantee that we will respond to all matters in the way that you might wish, we will strive to handle the matter fairly and properly. By using these Raising Concerns arrangements you will help us to achieve this.

A copy of the Whistleblowing (Raising Concerns) Policy is available on GTCNI's shared M Drive at M:\HUMAN RESOURCES for STAFF\STAFF POLICIES.

Appendix 5 - Guidance on Performing an Assessment of Fraud Risks

This appendix provides guidance on how to perform an assessment of fraud risks using the DE template provided below for a high level fraud risk assessment.

Fraud Risk Analysis - Guidance Notes.docx

Fraud Risk Analysis - Template.xlsx

Appendix 6 - Summary of Good Practice Guidance - Communicating With Staff

This guidance was developed to encourage the promotion of an anti-fraud culture within GTCNI.

Examples of how we will do this include:

- All Employees will undertake fraud awareness training.
- Making the anti-fraud policy and fraud response plan available to all staff and ensuring all staff confirm they have read and understood it.
- Regular updates on any key changes to fraud policy/response plans will be communicated to staff via networked IT systems.
- GTCNI will report to staff and publicise the outcomes of fraud investigations and the disciplinary action/prosecutions against employees who perpetrate theft or fraud.