

## Anti-Fraud Framework

<b>Version Number</b>	2
<b>Revision Date</b>	September 2023
<b>Department</b>	Strategic Finance
<b>Author</b>	Director Strategic of Finance
<b>Reason for Policy creation/revision</b>	Updated section on Anti Bribery and Anti Money Laundering
<b>Data Protection</b>	The impact of Data Protection has been assessed when considering our people and our customers
<b>Equalities</b>	The equality of opportunities for our people and customers has been considered in devising this policy
<b>Sustainability</b>	N/A
<b>Proof Read By</b>	Director of Business Support and Transformation
<b>Date Approved</b>	28 September 2023
<b>Approved by</b>	SMT
<b>Next Review Due</b>	March 2025
<b>Audience – Training and Awareness Method</b>	The regulation document will be briefed to our Senior Management Team and Operation Management Team as well as our Finance Business Partners providing training to our Budget Holders
<b>Effective Date</b>	12 October 2023
<b>Internal References – Policies &amp; Procedures (Located on Intranet)</b>	<p>ICT Code of Conduct</p> <p>Financial Regulation Documents</p> <p>Scheme of Delegation</p> <p>Whistleblowing Policy</p> <p>Cyber Security Management System</p> <p>Tenancy Management Policy</p> <p>Allocations Policy</p> <p>Procurement Plan</p> <p>Contract Management Framework</p> <p>Entitlements Payments &amp; Benefits Policy &amp; Procedure</p> <p>Fraud Response Process</p> <p>Board Code of Conduct</p> <p>Employee Code of Conduct</p> <p>Rights of Succession to a Tenancy for Scottish Secure Tenants</p> <p>Assignment, Subletting, Taking a Lodger and Mutual Exchanges</p> <p>Joint Allocations</p>
<b>External References</b>	The Fraud Act 2006

	Public Interests Disclosure Act Money Laundering, Terrorist Financing and Transfer of Funds Regulation 2017 Bribery Act 2010
--	---

## 1. Framework Purpose

- 1.1 Hanover is committed to achieving the highest standards of openness, probity and accountability and recognises the importance of this as it works to maintain its reputation and that of the wider housing sector.
- 1.2 This Anti-Fraud Framework is intended to support the development of a culture which raises the awareness of the risks and consequences of fraud. Appropriate actions will be taken to identify and guard against any adverse financial and business risks with a view to reducing its risk of fraud to the lowest possible level.
- 1.3 This framework provides a definition of fraud and outlines the principles Hanover will adopt to protect itself, any public monies it receives, its assets and its services against fraud.

## 2. Context and Definition

- 2.1 The Fraud Act 2006 defines fraud as: **““Loss” which includes a loss by not getting what one might get, as well as a loss by parting with what one has. A person is guilty of an offence if he has in his possession or under his control any article for use in the course of or in connection with any fraud.”**
- 2.2 Fraud is used to describe acts such as deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts, money laundering and collusion. For practical purposes, fraud may be defined as the use of deception with the intention of obtaining an advantage, avoiding an obligation, or causing loss to another party. The criminal act is the attempt to deceive, and attempted fraud is therefore treated as seriously as accomplished fraud.

## 3. Framework Scope

- 3.1 This Framework is relevant to Board, employees, customers, members of the public, contractors, consultants and service providers and it aims to put emphasis on the importance of deterring fraud. It provides details on the responsibilities placed on employees to identify and report any suspicion of fraudulent activity. (**Appendix 1 – Roles & Responsibilities**). The types of fraud that could be applicable to Hanover are detailed in the rest of section 2 below.
- 3.2 **Cyber fraud** is where technology equipment or data has been used to manipulate programmes or data dishonestly (for example, by altering, substituting, destroying records, or creating spurious records), or where the use of an IT system was a factor in the perpetration of fraud. Theft or fraudulent use of computer time and resources, including excessive personal browsing on the internet, is included in this definition.
- 3.3 Hanover has an ICT Code of Conduct which all employees should sign up to on an annual basis. This reflects the expectations that Hanover has for the correct use of its IT hardware and software. There are detailed policies and procedures for other elements that build towards a secure IT infrastructure (e.g., password policy, access restrictions, external access via VPN, spam filtering and firewall). Hanover is working to build a Cyber Security management system with the external validation of Cyber Essentials, Cyber Essentials Plus and in 2023 ISO27001 certification.
- 3.4 **Tenancy fraud** occurs when a property let by Hanover is occupied by someone who is either not legally entitled to be there or has obtained use of the property fraudulently. Common examples include application fraud, key selling fraud, subletting fraud and succession fraud. The means we employ to mitigate the risk of this type of fraud are detailed in policies maintained by Customer Services specifically:

- Rights of Succession to a Tenancy for Scottish Secure Tenants
- Assignment, Subletting, Taking a Lodger and Mutual Exchanges
- Joint Allocations

3.5 **Procurement Fraud** can happen when the tender process has not been followed so that fraud can be committed, or when there is bid rigging. It can also happen when there are payment claims for goods or services that were not delivered or were inferior to what was specified in the order. The Hanover Procurement Plan and Contract Management Framework are being developed to ensure procurement fraud does not take place.

3.6 The **Bribery Act 2010** explains that bribery is a criminal activity and is explained as a financial or other enticement or reward for action which is illegal, unethical, a breach of trust or improper in any way. Bribes can take the form of money, gifts, loans, fees, hospitality, services, discounts, contract awards or other advantage or benefit. Bribery includes offering, promising, giving, accepting, or seeking a bribe. Corruption is the abuse of entrusted power or position for private gain. There is an Entitlements Payments & Benefits Policy and procedure for recording any Gifts and Hospitality offered or accepted. Hanover prohibits Board Members, employees, or associated person from any of the following:

- Accepting a payment in cash if a contract is awarded to the contractor/supplier
- Accepting cash or an incentive from a customer to obtain access to housing or services
- Accepting an unusually generous gift or lavish hospitality
- Providing a supplier with an invoice receipt where no money is payable or has been paid;
- Accepting cash from a contractor cash to provide employment for a friend or relative;
- Accepting an invoice for an amount which seems large given the service/goods which have been provided;
- Receiving discounted fees for supply of goods to you as a private person.

This is not exhaustive list of examples of bribery but provide a flavour for types of bribe that could be offered to an organisation like Hanover. Any offers like this must be reported via the Fraud Response Process as detailed in **Appendix 2**.

3.7 **Money laundering** is the process by which funds derived from criminal activity are given the appearance of being legitimate by being exchanged for clean money. That means that the proceeds of any acquisitive crime are 'cleaned up' by various means and then fed back into the financial system after a transaction or series of transactions designed to disguise the original source of the funds. It also covers money, however come by, which is used to fund terrorism.

3.8 Money laundering can take a number of forms:

- Handling the proceeds of crime;
- Being directly involved with criminal or terrorist property;
- Entering into arrangements to facilitate laundering of criminal or terrorist property; Investing the proceeds of crime into other financial products, property purchase or other assets.

3.9 The Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017 ('the Regulations') came into force on 26 June 2017 and lists certain business activities, including some types of business undertaken by housing associations. These include:

- Letting of social housing

- Factoring of owners homes
- Procurement of new homes
- Property disposals

3.10 Hanover has robust policies in place and active risk management practices that ensure that any risks attached to the above areas are mitigated and managed as much as possible. For letting and factoring risks, robust identity checks and rigorous processes are in place for the commencement of new tenancies. For the procurement and disposal of properties that could be the basis for money laundering third party's such as solicitors would be used to ensure due diligence was followed and to transact any funds to and from.

## Framework and Principles

4.1 Hanover recognises the potential for fraudulent activity to take place within the business or targeting an area of the business. Its responses to the threat of fraud are to embrace recognised good practice and adhere to an anti-fraud culture through the following:

- A zero-tolerance approach to fraud.
- Ensure any allegation of fraud, anonymous or otherwise will be investigated.
- Have a consistent approach when dealing with cases without regard to the position held or the length of service.
- Give consideration as to whether there have been failures in supervision.
- Prevent fraud by eliminating weaknesses out of policies, processes and systems.
- Detect fraud where it cannot be prevented.
- Pursue recovery for any losses incurred, if necessary, through civil action.
- Creating a strong deterrent effect.
- All frauds will be reported to the police.
- A review after any investigation to ensure lessons are learned.

4.2 Central to the framework are a range of operational policies, systems and procedures that are designed to deter, and enable the detection of fraud. Key documents include:

- The Financial Control Framework incorporating The Financial Regulations Documents, Financial Policies and Financial Procedures and all the controls contained therein.
- The Rules, The Scheme of Delegation, The Good Governance Guide and other governance related policies, policies around whistleblowing, gifts, and hospitality, employees' benefits, notifiable events, conflicts of interest and any associated management systems.
- Service based policies, guidance and operating procedures covering tenancy related matters; repairs, maintenance, and development activities; estates services and employees' recruitment.

4.3 There is a commitment to maintaining an honest and open environment within Hanover and a commitment to eliminate any fraud. Rigorous investigations will be undertaken if there are any such cases. This is done by monitoring the existence of and adherence to the Fraud Response Process (**Appendix 2**)

4.4 If any employee or Board member has reasonable suspicions of fraud, they need to report them as outlined in the Fraud Response Process. It is therefore also policy, which will be rigorously enforced, that no employee will suffer in any way as a result of reporting reasonably held suspicions. For these purposes, reasonably held suspicions shall mean any suspicions other than those which are raised maliciously and found to be groundless. The business will deal with all incidents in accordance with the Public Interest Disclosure Act which protects whistle-blowers from detrimental treatment by their employer as aligned with our Whistleblowing Policy.

4.5 Established Internal Audit arrangements further support the detection of fraud, through testing the appropriateness, adequacy, effectiveness and robustness of relevant policies, processes, and systems. Similarly, through the annual examination of the financial statements, the External Auditor identifies any audit and accounting issues and assesses the effectiveness of internal controls.

## **5. Monitoring & Evaluation**

5.1 This framework will be monitored by the Director of Strategic Finance who will ensure:

- That roles and responsibilities in relation to the Anti-Fraud Framework are understood and being maintained.
- The Fraud Response Process is actioned.
- Ensuring the reporting requirement in relation to any suspected fraud are executed.

## **6. Review**

6.1 The Anti-Fraud Framework will be reviewed every three years or earlier as required by a change in best practice or legislation.

## Appendix 1 - Roles and Responsibilities

### 1. The Board

- 1.1 The Audit, Performance & Risk Committee is responsible for ensuring there is a robust and up to date Anti-Fraud Framework in place and that this regulation document and its related procedures are regularly reviewed and kept fit for purpose. The Director of Strategic Finance monitors this and updates the Committee on any investigations.
- 1.2 The Board members are responsible for following the Board Members Code of Conduct.
- 1.3 The Board is also responsible for ensuring it conducts its own affairs in accordance with the Scottish Housing Regulator's regulatory standards of governance and financial management, and recognised principles of good governance. Individual Board Members are responsible for reporting any suspicions of fraud or attempted fraud they encounter, and otherwise acting with integrity and propriety, within the law, and in accordance with relevant policies and procedures.

### 2. The Executive Leadership Team

- 2.1 The Executive Leadership Team are responsible for:
  - Developing and maintaining the Anti-Fraud Framework by ensuring effective policies, procedures, and control systems for deterring, detecting, and reporting fraud are in place. Ensuring these are working effectively and are periodically reviewed in accordance with good practice.
  - Reported incidents of suspected fraud are promptly and vigorously investigated; and effective sanctions and redress are applied in instances where fraud is detected.
  - Ensuring employees have up to date and accurate information on regulatory requirements in relation to governance and financial management, governance good practice and expected standards of conduct.
  - Fostering a culture of honesty and openness amongst all employees, and ensuring employees are aware of expectations relating to their professional conduct and the requirements of this framework.
  - Ensuring all employees have the required level of knowledge and understanding of the range of policies, procedures and systems that are relevant to the Anti-Fraud Framework.
  - Implementing any relevant operational anti-fraud measures, including segregation of duties.
  - Ensuring employees receive appropriate training that enables them to identify suspected fraud.
  - Ensuring the notification requirements of regulators are met.
  - Effective risk management and internal control system are in place.

### 3. The Director of Strategic Finance

- 3.1 In addition to the responsibilities listed above, the Director of Strategic Finance is the first point of contact when reporting a fraud or a suspected fraud.
- 3.2 The Director of Strategic Finance is responsible for ensuring the Fraud Response Process (**Appendix 2**) is used and followed when a fraud has occurred or there is a suspicion that a fraud has occurred.
- 3.3 Ensuring that the Fraud Response Process is up to date and fit for purpose is the responsibility of the Director of Strategic Finance.

## 4. Heads of Service and Managers

4.1 The responsibility for the prevention and detection of fraud rests primarily with our managers. Therefore, there is a need for all managers to:

- Assess the types of risk involved in the operations for which they are responsible.
- Develop systems of internal control to minimise the risk of fraud.
- Ensure controls are being consistently applied; this will include testing the controls and maintaining a record of all such tests.
- Satisfy themselves that their systems continue to operate effectively.
- Provide assurances on their internal control systems.
- Raise fraud awareness amongst employees including knowledge of the Anti-Fraud Framework.
- Ensure that the Director of Strategic Finance is informed when a fraud has occurred or is suspected.
- Implement new controls to reduce the risk of similar fraud occurring where frauds have taken place.

4.2 The ICT Manager is responsible for the process for cyber fraud and maintains a disaster recovery plan.

4.3 The Head of Enhanced and Head of Care are responsible for the process for tenancy fraud and maintaining a tenancy anti-fraud plan.

4.4 Managers must ensure that the opportunities for employees to commit fraud are minimised. In establishing and maintaining effective controls, it is desirable that:

- Where practical, there is rotation of employees.
- Where possible, there is separation of duties so that control of a key function does not rest with one individual.
- Ensure backlogs are not allowed to accumulate especially in relation to tasks such as Bank Reconciliations and the matching of Credit Card Statements with receipts.
- Employees are trained and have available to them relevant documented procedures.

4.5 As regards the personal conduct of employees, managers should:

- Ensure that Employees under their management have read and understood the content of the Employees Induction Guide and other employees related policies.
- Ensure that Employees under their management have read and understood the content of the ICT Conditions of Use.
- Encourage Employees to make internal disclosure of behaviour that could be deemed as negligent or inappropriate.
- Ensure that Employees under their management are aware of the rules relating to confidentiality of information and GDPR procedures.
- Ensure that Employees under their management have been aware that fraudulent behaviour is wrong and are aware of the consequences of involvement in fraudulent activity.
- Ensure Tender Evaluation Panellist Conflict of Interest Declaration forms are signed for all Employees and external consultants assessing tender returns.
- Ensure that bidders have completed the Declaration, Conflict of Interest Statement and Certificate to Tender and signed as part of any tender return.
- Ensure that all Employees record all gifts and hospitality received within the Register of Gifts and Hospitality in the required format.
- Regular reinforcement of the rule relating to personal conduct.



4.6 When dealing with a suspected fraud, managers, in consultation with the Executive Team and the Investigating Officer, will examine the necessity to suspend the member of employees to ensure that all original documentation is preserved in a safe place for further investigation.

## **5. Employees Responsibilities**

5.1 Every employee has a duty to ensure that Hanover's assets are safeguarded whether they are involved with cash or payments systems, receipts, stocks or dealing with suppliers or contractors. Employees must have a high standard of personal integrity.

5.2 Employees should:

- Alert their manager where they believe the opportunity of fraud exists because of poor procedures or lack of effective supervision.
- Report details immediately to their manager or next most senior person if they suspect that a fraud has been committed or see suspicious acts or events.
- Assist in any investigations by making available relevant information and by co-operating in interviews.
- Inform management of any outside interest which might impinge on their discharge of duties – through the annual employees' declaration system.
- Record any gifts, hospitality or benefits of any kind received from a third party as detailed within the 'Conditions of Service and Employees Rules.' In line with the Payments and Benefits policy
- Where Cyber Fraud is suspected, employees are requested to immediately stop and report any unusual activity to a member of the ICT department.

## Appendix 2 – Fraud Response Process

### 1. Introduction

- 1.1 The purpose of the Fraud Response Process is to outline the steps to be followed in the event of a suspected fraud. It provides a consistent framework for investigating and reporting fraud by defining authority levels, responsibilities for action and lines of reporting. This Process should be used in conjunction with the Anti-Fraud Framework, the Investigation Procedure, and the Whistleblowing Policy.
- 1.2 In the event that fraud is suspected the following processes need to be followed through:
  - Notifying suspected fraud.
  - The investigation processes.
  - Liaison with police, internal and external audit.
  - Initiation of recovery action.
  - Reporting process.

The details of these processes are in the sections which follow.

### 2. Notifying Suspected Frauds

- 2.1 It is important that all employees can report their concerns without fear of reprisal or victimisation and are aware of the means to do so. Hanover's Whistleblowing Policy provides appropriate protection for those who voice genuine and legitimate concerns through the proper channels.
- 2.2 In the first instance, any suspicion of fraud, theft or other irregularity should be reported to the Director of Strategic Finance as a matter of urgency. If such action would be inappropriate, concerns should be reported to one of the following persons: Other Directors, Chief Executive or Board Members.
- 2.3 Every effort will be made to protect an informant's anonymity if requested. In certain circumstances, anonymity cannot be maintained. This will be advised to the informant prior to release of information.

### 3. The Investigation Process

- 3.1 The investigation process will vary according to the circumstances of each case and will be determined by the Director of Strategic Finance. An 'Investigating Officer' will be appointed to take charge of the investigation on a day-to-day basis. This investigation will follow the guidelines detailed in the Investigation Procedure.
- 3.2 The Director of Finance will enact the investigation process in relation to an alleged fraud to ensure that:
  - Regulatory Standards are followed, and The Scottish Housing Regulator is informed.
  - The correct process for informing the Scottish Housing Regulator for a 'notifiable event' is followed.
  - The Audit, Performance & Risk Committee are informed that, and investigation is to be undertaken and the Scottish Housing Regulator has been informed regarding the notifiable event.
- 3.3 The findings of the investigation will be reported to the Director of Strategic Finance who will determine, in consultation the Executive Team and the Investigating Officer, what further action (if any) should be taken.

#### **4. Liaison with Police and Internal / External Audit**

- 4.1 The police welcome early notification of suspected fraud, particularly that of a serious or complex nature. Some frauds will lend themselves to automatic reporting to the police (such as theft by a third party). The Director of Strategic Finance will report suspected frauds to the internal / external auditors at an appropriate time.
- 4.2 All employees must co-operate fully with any police or internal / external audit enquiries, which may have to take precedence over any internal investigation or disciplinary process. However, wherever possible, teams will co-ordinate their enquiries to maximise the effective and efficient use of resources and information.

#### **5. Initiation of Recovery Action**

- 5.1 Appropriate steps including legal action will be taken, if necessary, to recover any losses arising from fraud, theft, or misconduct. This may include action against third parties involved in the fraud or whose negligent actions contributed to the fraud.

#### **6. Reporting Process**

- 6.1 Throughout any investigation, the Investigating Officer will keep the Director of Strategic Finance informed of progress and any developments. If the investigation is long or complex, interim reports may be made to the ELT. These reports may be verbal or in writing depending on the seriousness and material nature of the suspected fraud.
- 6.2 On completion of the investigation, the Investigating Officer will prepare a full written report setting out:
  - Background as to how the investigation arose.
  - What action was taken in response to the allegations.
  - The conduct of the investigation.
  - The facts that came to light and the evidence in support.
  - Action taken against any party where the allegations were proved.
  - Action taken to recover any losses.
  - Recommendations and / or action taken by management to reduce further exposure and to minimise any recurrence.
- 6.3 A copy of the above report will be submitted to the ELT and Audit, Performance & Risk Committee (if required).
- 6.4 The incident will be logged within the Fraud Register. This register is reviewed regularly by the Strategic Finance Director and is open to regulatory inspection. The external auditors will review this register as part of their normal audit work and will be signed off annually by the Chair.
- 6.5 In order to provide a deterrent to other employees, a brief and anonymised summary of the circumstances will be discussed at team meetings.

#### **7. Lessons Learned**

- 7.1 Where a fraud has occurred, management must make any necessary changes to policies, processes, and systems to ensure that similar frauds will not occur. Hanover's internal auditors can offer advice and assistance on matters relating to internal control, if considered appropriate.

## **8. Review of Fraud Response Process**

- 8.1 As a minimum the Fraud Response Process will be reviewed every three years to ensure it is fit for purpose. It should also be reviewed after any instance of fraud or incident to identify any need for change.