|  |
| --- |
|  |
| **Fraud, Bribery and Corruption Policy**  **COR-POL-10**  **Version 4.1** |
| **Date approved: 25th July 2023**  **Approved by: Audit and Risk Committee** |

# Introduction

* 1. Southway Housing Trust (Southway) promotes ethical behaviour and high standards of probity. We have a moral responsibility to make the best use of our resources to deliver our objectives, improve the lives of our tenants and build stronger communities.
  2. We recognise that any involvement in fraud, bribery or corruption will reflect adversely on our image and reputation amongst residents and stakeholders and could prevent us from delivering services to our Community. This Policy explains Southway’s approach to the prevention and detection of fraud, bribery and corruption.
  3. This Policy applies to all employees, Board and Committee Members, involved tenants and volunteers, contractors and partners of Southway Housing Trust and any of its subsidiary companies. Partners and contractors will be sent a copy of this Policy and will be required to sign their agreement to adhere to it prior to their appointment.
  4. There are several pieces of legislation relating to fraud, bribery and corruption that have been taken into account when writing this Policy. They are listed, with a brief explanation of their relevance, at Appendix B.

# Definitions

* 1. **Fraud**

A fraud occurs where a person wilfully assists in the misdirection of another party’s money or property for the benefit of themselves or an acquaintance.

The Fraud Act 2006 focusses on the dishonest behaviour of the suspect and their intent to make a gain either for themselves or another; to cause a loss to another; or, expose another to a risk of a loss.

The offences of fraud can be committed in three ways:

1) Fraud by false representation (s.2) – lying about something using any means, e.g. by words or actions

2) Fraud by failing to disclose (s.3) – not saying something when you have a legal duty to do so

3) Fraud by abuse of a position of trust (s.4) – abusing a position where there is an expectation to safeguard the financial interests of another person or organisation.

* 1. It should be noted that all offences under the Fraud Act 2006 occur where the act or omission is committed dishonestly and with intent to cause gain or loss. The gain or loss does not have to succeed, so long as the intent is there. Some examples of potential fraud that could affect Southway include, but are not limited to:

# Cybercrime

# The taking of a bribe that affects a decision over resources

# Conspiring with another party to misdirect Southway’s property

# Invalidly signing documents or making false statements which affect the direction of Southway’s property

# Covering up a previous act or attempt at fraud

# Misallocation of properties

* Misuse of Company Vehicles
* Dishonestly claiming for additional hours or overtime.

Theft issues come under the Theft Act 1968, where potential criminality is identified this will be dealt with in line with investigations of fraud.

* 1. **Bribery and Corruption**

Bribery and corruption is the offering, promising or giving of a financial or other advantage designed to induce an individual to take an improper decision or action.

The persons making and receiving the bribe may be acting on behalf of others – under the Bribery Act 2010, all parties involved may be prosecuted for a bribery offence.

Bribery does not have to involve cash or an actual payment exchanging hands and can take many forms such as a gift, receiving lavish treatment during a business trip or tickets to an event.

* 1. Southway strictly prohibits the offering, giving, solicitation or acceptance of any bribe whether cash, or other form:
* To or from any person or Company, wherever they are based, whatever their relationship with Southway, and whether they are a foreign public official, body, private person or company,
* By any individual employee, Board Member, partner, contractor, agent, person or body acting on behalf of Southway,

In order to:

* Gain any commercial, contractual, strategic, social or regulatory advantage for Southway in a way which is unethical, or
* Gain any personal advantage, pecuniary or otherwise, for the individual or anyone connected with the individual.

All staff and Board Members are reminded to be transparent in recording any gifts, hospitality or sponsorship. They should refer to the Code of Conduct which includes details on the policy for Gifts and Hospitality.

# Southway’s Approach to Tackling Fraud

* 1. Southway has a three-pronged approach to tackling fraud and bribery, which is explained in the following sections of the Policy:
* Promotion of an Anti-Fraud Culture
* Systems of Prevention
* Investigation and Action

# Promotion of an Anti-Fraud Culture

* 1. Southway is a values-based organisation. We take responsibility for our actions, are open with our stakeholders and can be trusted to do the right thing.’ This underpins our organisational approach to tackling fraud.
  2. Southway does not tolerate fraud, bribery or corruption and aims to eliminate all such activity. Southway undertakes thorough reference checks of all prospective employees and Board Members to ensure that they do not have a history of perpetrating fraud.
  3. Most fraud attempts are defeated by human intervention. All staff are required to report any reasonable suspicions of fraud, bribery or corruption immediately (see section 6 and Appendix A).
  4. All newly inducted staff and Board Members will be given guidance on how to report a suspected fraud. Refresher training will be provided to all staff at least once every 3 years.
  5. Staff who are involved in transactions that involve receiving large payments from customers, tenants and shared owners will be given specific training on the prevention of money laundering. See Southway’s Anti- Money Laundering Policy for further detail.
  6. Staff and Board Members sign an annual Declaration of Interests Form. This covers key potential areas for fraud, bribery and corruption including allocation of housing, procurement of goods and services, relationship with customers, and gifts and hospitality. The Code of Conduct is reviewed at least every 3 years to ensure that it is robust, and clear to those who are subject to it.
  7. Southway never makes donations in the anticipation of direct advantage to itself or any of its staff.
  8. Staff are expected, in the first instance, to reject any offers of gifts or hospitality that they receive from partners, contractors and tenants. If this is not possible, they must advise their line manager. If the gift is over £10 they should report this to the Head of Corporate Services who will make an entry on the Gifts and Hospitality register and provide advice on how to proceed.
  9. This Policy is not meant to prohibit the following practices providing they are proportionate and are properly recorded:
* Donations and sponsorship, or
* Offering a free (or reduced charge) service as an informal marketing tool, provided it creates no formal expectation on the other party.
  1. If anyone is in doubt as to whether a potential act constitutes bribery, the matter should be referred to the Head of Corporate Services, or another member of the Executive Group who will provide guidance.
  2. To ensure that data is not lost, which could then potentially be used as an incentive for a bribe, all staff will be given appropriate training. Any ICT hardware that is taken into the field will have the necessary encryption to protect personal and sensitive personal data. The ICT Network Security Policy and Personal use of ICT Equipment Policy provide more detail.

# Systems of Prevention

Responsibilities

* 1. Under Southway’s Group Standing Orders, the Audit and Risk Committee are delegated to:

‘*Ensure that the impact of alleged or fraudulent activity on the organisation’s framework of internal control is properly assessed and, where it considers it necessary, to recommend changes to strengthen the control framework.*

*To receive reports relating to any matters of whistleblowing or alleged or actual fraudulent activity that may have an effect upon the organisation (or any of its subsidiaries) and ensure that any necessary reports about fraud are made to the Regulator’*

* 1. The Chief Executive has a responsibility to protect and advance the interests of Southway and ensure that Directors and their operational managers design all management arrangements and control systems that prevent the risk of fraud, bribery and corruption. There are certain officers with specific responsibilities listed below.
  2. The Chief Financial Officer is responsible for ensuring that all financial systems are robust and cannot be easily exploited so that fraud can be committed.
  3. According to Office of National Statistics Data from September 2022 around 60% of reported fraud is cybercrime. The Head of ICT is responsible for ensuring that the technology Southway uses is resistant to fraud and is regularly tested.
  4. The Head of Corporate Services responsible for the co-ordination of fraud investigations, arranging training, and submitting the annual report to the Regulator. They also report any significant events or ‘near misses’ to the Audit and Risk Committee as part of the annual Internal Controls Assurance Report.
  5. The Head of HR is responsible for the relevant pre-employment checks. The Head of HR will consider any reference requests from former Southway Officers, found to have committed fraud, with due regard for prevailing employment law.
  6. Southway has several policies, procedures and internal controls designed to minimise the risk of fraud. These include, but are not limited to:
* The Financial Regulations, which set out clear divisions of authority for incurring and authorising expenditure.
* Internal controls that minimise the risk of fraud in the setting up of new suppliers and authorising payments to suppliers.
* A Policy on Gifts and Hospitality reflected in the Codes of Conduct, which are reviewed and signed by each individual every year.
* A range of ICT policies and procedures, which are reviewed on a regular basis, designed to mitigate the increasing risk of cyber-fraud.
* Annual Penetration Testing of Southway’s networks.
* Clear records of Southway’s finances, declarations of interests, gifts and hospitality, donations and procurement, which can be made available to appropriate parties upon request.
* Procedures to ensure that any consultants employed directly by Southway Housing Trust or its subsidiaries, any Southway Housing employees with secondary employment, or any company supplying goods and services to Southway is not involved in tax evasion.

# Investigation and Action

* 1. Southway will robustly investigate any reports of fraud, bribery and corruption and will take timely, appropriate and proportionate action. We recognise that where fraud is suspected, or detected, the quality of the response may act as a deterrent to future occurrences.

**Reporting**

* 1. A member of the Senior Management Team or a Board Member who has reasonable suspicions of fraud or who has been advised of such suspicions must notify the Head of Corporate Services immediately.
  2. Employees who are not members of the Senior Management Team must, in the first instance, report their suspicions to their line manager. That employee is entitled to seek written confirmation that their suspicions have been conveyed by that manager to the Head of Corporate Services..
  3. Where an employee has suspicions which wholly or partly relate to someone who they would normally be expected to report the matter to, then that person may be bypassed in the process. (So, for instance, if they believe that their own manager is implicated an employee can go straight to the Head of Corporate Services)
  4. The Internal and External Auditors, where appropriate, will notify the Head of Corporate Services of any suspicions they have. These parties also have the right to notify the Chair of the Audit and Risk Committee directly.
  5. The Head of ICT is responsible for ensuring that they notify the Head of Corporate Services in all cases where there is suspicion that Southway ICT (Information and Communications Technology) is being used for fraudulent purposes in accordance with the Computer Misuse Act 1990.
  6. Southway’s Whistleblowing Policy gives further guidance on how to report concerns and the support that is available. Confidentiality for all parties will be maintained over reports made in good faith where no action can be taken following investigation.

## Investigation

* 1. The Head of Corporate Services has overall responsibility for resolving any issues of suspected fraud and will decide upon the scope and practicalities of an investigation, including assigning a lead officer or officers where appropriate and ensuring that investigations are dynamic. In the absence of the Head of Corporate Services, the Chief Executive will make arrangements for the incident to be investigated.
  2. Where an allegation involves a Board Member or a member of the Senior Management Team the Chief Executive will lead the investigation. Reference will be made to Financial Regulations in the Chief Executive’s absence.
  3. Where values exceeding £10,000 are involved, the Internal Auditor will be consulted on who should investigate. Where the Internal Auditor and the Head of Corporate Services disagree, the Internal Auditor will seek the direction of the Chair of the Audit and Risk Committee, whose decision will be final.
  4. The Head of Human Resources will provide specialist advice and operational support as required, including liaison with the appointed investigator, and instigating the necessary disciplinary action against those where it had been identified that they have failed to comply with the policies, procedures and processes of Southway.
  5. The Head of Corporate Services will produce and maintain a Fraud Register to record all relevant significant events. These will include:
* The initial recording of each allegation, as soon as there is reasonable evidence,
* Any subsequent reasoned allegations and findings on the case,
* The names of the parties notified (and date notified), and
* Key events of the investigation, and the parties conducting it

6.12 The Head of Corporate Services will brief the Chief Executive prior to the commencement of the investigation and will update them at regular intervals throughout, in particular when any new information is received.

6.13 Should either the Chief Executive or the Head of Corporate Services be unavailable for a prolonged period when a fraud is reported, then reference will be made to Financial Regulations to resolve how to progress the investigation. A procedure explaining how to conduct an investigation is included at Appendix A of this Policy.

## Notification

6.14 The Chair of the Audit and Risk Committee will be notified as soon as there is reasonable suspicion that a sum of more than £1,000 may be involved.

6.15 The Audit and Risk Committee will be notified of all entries made in the Fraud Register since its previous meeting and will be notified as soon as there is reasonable suspicion that a sum of more than £10,000 may be involved. The only exception is where, in the opinion of both the Head of Corporate Services and the Chair of the Audit and Risk Committee, this would impair the investigation.

6.16 The Regulator will be notified in accordance with prevailing Regulatory Guidance.

6.17 The Internal and External Auditors will be notified of all entries, over £1000 in the Fraud Register within five working days. They will be notified immediately of suspicions of fraud where in the opinion of the Head of Corporate Services these are considered to be reasoned.

6.18The Police will be notified by the Head of Corporate Services where:

* The suspicion is considered to be reasoned and may involve a value exceeding £10,000, or
* The Head of Corporate Services and the Chair of the Audit and Risk Committee, in consultation with the Chief Executive, perceive that the value involved does not exceed a value of £10,000 but the adoption of criminal investigation processes would be in Southway’s interests, or
* Where there is reasonable suspicion that the incident may be part of a wider fraud affecting parties not formally connected to Southway.

6.19The Insurance Broker will be notified in accordance with any Fidelity Guarantee Policy taken out from time to time.

* 1. The Press

No aspect of any allegation or any subsequent investigation may be disclosed to the press except by the Chief Executive, who will act in consultation with the Chair of the Board. Where the Police have been involved, disclosures will only be made by the Chief Executive following consultation with them.

# Related Policy Documents

* Treasury Management Policy
* Financial Regulations
* Group Standing Orders
* Shareholder Admission Policy
* Anti-Money Laundering Policy
* Data Protection and Information Sharing Policy
* Whistleblowing Policy
* Probity Policy
* Code of Conduct (Board)
* Code of Conduct (Officers)
* Disciplinary and Capability Policy
* ICT Information Security Policy
* ICT Policy
* Personal use of ICT Equipment Policy
* Allocations Scheme

|  |  |
| --- | --- |
| **POLICY REVIEW HISTORY** | |
| *To be completed during each review* | |
| **Previous versions**  (version number – approved by – approval date – title if different)  Fraud  V1 – Shadow Board – 09/10/2007 – Anti-Fraud and Counter Corruption Policy  V2 – Board – 03/11/2009 – Anti Fraud Policy  V2.1 – Audit and Risk Committee – 11/10/2011 – Fraud Management Policy  V3.0 – Audit and Risk Committee – 21/04/2015 – Fraud Management Policy  V3.1 – Chief Executive – 21/03/2017 – Fraud Management Policy  V3.2 – Audit and Risk Committee – 17/10/2017 – Fraud Management Policy  V3.3-Chief Executive-November 2018  V4 Audit and Risk Committee October 2019  Bribery  V1 – Audit and Risk Committee – 11/10/2011 – Bribery Policy | |
| **Date of last EIA:** | N/A |
| **Review lead by:** | Matthew Maouati, Head of Corporate Services |
| **Main points or amendments made and reasons**   * Renaming the policy Fraud, Bribery and Corruption * Updating definitions contained in the Fraud Act and Bribery Act and removing some examples which are not relevant-Section 2 * Change in procedure for gifts and hospitality under £10 * Commitment to reporting near misses to the Committee on an annual basis-5.5 * Adding reporting obligations to the Head of ICT relating to the Computer Misuse Act 1990-6.6 * Linking fraud investigation to disciplinary action where appropriate-6.12 | |
| **Next review due:** | **Quarter 3 2025/26** |
| **Approval level:** | **Audit and Risk Committee** |

**Appendix A**-Fraud Investigation Procedure

1. Where an investigation is conducted internally, the investigator(s) will be people who, in the opinion of the Head of Corporate Services is/are:

* Competent in relation to the nature of the allegations,
* Senior to the most senior person accused, and
* Not likely to be impeded by their personal and professional relations with those suspected.

1. The Head of Corporate Services will assess the degree to which the investigator(s) need to be independent of the processes through which the fraud may have taken place.
2. As soon it is perceived that the Police may be involved, or that the Regulator has directed on the conduct of an investigation, any investigations by internal officers or Internal Audit will be in accordance with their respective advice or directions.
3. The investigator(s) will be directed to immediately report significant findings to the Head of Corporate Services, who will then be obliged to consider updating (or initiating) disclosure to other parties.

1. A Fraud Response Plan will be produced. The investigator(s) will make disclosures only in accordance with the Fraud Response Plan for the case. This Plan will restrict the investigators’ reporting lines to the Head of Corporate Services and the Chief Executive, or others expressly advised by those officers. Exceptions may be required where the Police or the Regulator have directed the investigation, and this will be reflected in the Plan.
2. Investigations will balance the need to uncover the truth with the need to protect against the risk that subsequently unfounded allegations might nevertheless tarnish the accused.
3. The investigator(s) will always be asked to advise findings which might indicate the need for action under Disciplinary or Capability Policies. These actions may be for the fraud itself, or for related matters (such as breach of procedure, dereliction of duty, or incompetence).
4. The timing of such action will take account of the requirements for fairness and timeliness under employment law, and of the needs of any actual or potential Police investigation.
5. Where losses have been sustained, the Plan will consider if they can be recovered . Where this might be an involved process, legal advice will be taken on the cost / benefit..
6. Any weaknesses in systems of control identified during, or at the culmination of, an investigation will be addressed by the lead officer for the service area and will be supplemented by a Management Action Plan monitored by the Audit and Risk Committee. This is not dependant on an actual fraud being proved – belief that the fraud was simply possible may warrant immediate changes.

**Procedure for Reporting and Investigating a Fraud**

In the event of a known or suspected fraud

Head of Corporate Services completes a fraud register.

Assigns Lead Officer/s

Report to Line Manager

Support and advice will be provided from the Head of Human Resources

Head of Corporate Services decides whether fraud should be reported to police and/or regulator

If the fraud is <£10k, the Head of Corporate Services will consult with the Internal Auditor on the appointment of suitable officer/s

Report to the Head of Corporate Services

Head of Corporate Services reports to Chief Executive and will update and inform on progress

Head of Corporate Services notifies Internal and External Auditors

**Fraud Act 2006**

This Act sets out clear definitions of what constitutes fraud. There are three main offences:

* Fraud by false representation,
* Fraud by failing to disclose information, and
* Fraud by abuse of position.

The Act also created three new offences, including:

* Obtaining services dishonestly with intent to avoid payment, and
* Possessing making and supplying articles for use in frauds.

**Theft Act 1968**

Many of the relevant clauses of this Act were subsumed into the Fraud Act (see above). There are however specific sections relating to false accounting, false statements from Company Directors, and liability of company officers for certain offences.

**Computer Misuse Act 1990**

This Act means that a person can be guilty of a criminal offence if they use a computer to conduct an unauthorised act.

**Data Protection Act 2018**

Section 170 of this Act states that is an offence for a person to knowingly or recklessly,

(a)to obtain or disclose personal data without the consent of the controller,

(b)to procure the disclosure of personal data to another person without the consent of the controller, or

(c)after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

**Identity Documents Act 2010**

This Act means that it is an offence for a person with an improper intention to have in their possession or under their control:

* An identity document that is false and that they know or believe to be false,
* An identity document that was improperly obtained and that they know to have been improperly obtained, or
* An identity document that relates to someone else.

**Proceeds of Crime Act 2010**

The main offences in this Act relevant to Southway relate to money laundering namely:

* Concealing, disguising, converting, transferring or removing criminal property from the UK.
* Entering into or becoming concerned in an arrangement which facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person.
* Failing to disclose knowledge or suspicion of money laundering to the money laundering reporting officer (MLRO).

**Bribery Act 2010**

This Act introduced four separate offences:

* Active bribery-paying, offering or promising to give a bribe,
* Passive bribery-requesting, agreeing to receive or accepting a bribe,
* Bribery of a public official, and
* Failure of a commercial organisation to prevent bribery.

The Act does not prohibit corporate hospitality *per se* and actions taken must be proportionate to the risk of bribery within the organisation. The Act extended the liability of incidents to perpetrators’ employers in some instances.

**Corporate Criminal Offence of Failure to prevent the Facilitation of Tax Evasion 2017**

Based on the UK Bribery Act 2010, the legislation creates two new corporate offences of failure to prevent the facilitation of tax evasion – a domestic fraud offence and an overseas fraud offence. The aim of the legislation is to overcome the difficulties in attributing criminal liability to corporates for the criminal acts of ‘associated persons’ i.e. facilitating tax evasion. ‘Associated persons’ can include employees, contractors, agents or those that provide services for or on their behalf. Under the draft legislation, it is the corporate that is subject to prosecution without the need for prosecution of any individual.

**CRIMINAL FINANCES ACT**

This gives law enforcement agencies and partners, further capabilities and powers to recover the proceeds of crime, tackle money laundering, tax evasion and corruption, and combat the financing of terrorism.