RELIANCE SOCIAL HOUSING
GENERATE | ACQUIRE | DEPLOY



RELIANCE HOUSING ANTI-FRAUD & AML POLICY

Policy Checklist	
Policy Owner	CFO
Author	CFO
Version No.	1.3
Approved by Chief Executive	Yes
Approved by Board	Yes
Date of Implementation	September 2023
Date of Last Review	June 2026
Date of Next Review	June 2028

Contents:

1 Introduction

2 Definition of Fraud

3 Background

4 Reporting fraud

5 What is prohibited

6 Roles and responsibilities

7 Monitoring

8 Anti money laundering

9 Policy review

Appendices:

Appendix 1 Anti-Fraud and Anti Money Laundering Policy Summary

Appendix 2 Fraud, whistleblowing and notifiable events registered

1.0- Introduction

1.1 Fraud can have a devastating effect on a company because it could result in significant financial loss and other long-term business repercussions. Any allegations of fraud will be taken seriously, with no exceptions. All individuals, regardless of position, title, or tenure with the company are expected to remain vigilant and report any suspicious activity to the relevant staff member and/or the fraud prevention hotline.

1.2 These procedures promote a culture founded on fraud prevention, awareness, accountability and clarify acts that are suspicious. This will ultimately support a culture of operating within a comprehensive framework of internal controls, complete with documented and formalized policies, procedures, processes, and other supporting safeguards as needed. The procedures provide guidance to prevent, detect, report, and investigate when fraudulent acts are suspected and subsequently proven.

1.3 Reliance Social Housing CIC (RSH) upholds a zero-tolerance approach regarding fraud and corruption and is committed to achieving the highest standards of openness, probity and accountability. It identifies the importance of this as it works to preserve its reputation and that of the sector.

1.4 RSH will identify and promptly investigate any suspected fraudulent or related dishonest activity against the company or other parties with whom the organization has dealings. RSH will take appropriate disciplinary and legal actions to include the possibility of termination of employment, restitution, and forwarding information to the appropriate authorities for prosecution.

1.5 In pursuit of the aim to carry on a workable and sustainable business it takes appropriate actions to identify and guard against improper financial and business risks. RSH is committed to reducing its risk of fraud to the lowest possible level.

1.6 This policy outlines the broad principles which RSH will implement in order to protect the organisation and the public funds it receives, its assets and its services against fraud. It is relevant to Board and Committee Members, staff, tenants and residents, members of the public, contractors, consultants and service providers. , This fraud policy should outline RSH determination to take appropriate measures to deter fraud by:

- introducing/maintaining necessary procedures to detect fraud;
- Investigate all instances of suspected fraud;
- Report all suspected fraud to the appropriate authorities;
- Assist the police in the investigation and prosecution of suspected fraudsters.
- Recover wrongfully obtained assets from fraudsters
- Encourage employees to report any suspicion of fraud.
- You may also wish to include the following:
- the allocation of responsibilities for the overall management of fraud and
- procedures to be followed if a fraud is suspected.

2.0 Definition of Fraud

2.1 Fraud is any intentional act or omission designed to deceive others, resulting in the other

party suffering a loss and/or the perpetrator achieving a gain. Dishonest or fraudulent activities include, but are not limited to, the following:

- Forgery or alteration of documents (checks, bank draft, timesheets, invoices, agreements, etc.) or bank accounts belonging to the company or its subsidiaries.
- Misrepresentation of information on documents.
- Misappropriation of funds, supplies, or assets.
- Theft, disappearance, or destruction of assets.
- Authorizing or receiving payments for goods not received or services not performed.
- Authorizing or receiving payment for hours not worked.
- Inappropriate use of the company's records and disclosing confidential
- and proprietary information to outside parties
- Corruption is defined as the offering, giving, soliciting, or acceptance of an inducement or reward that may improperly influence the action of a person or entity. Some examples of corruption include:
    - Bribery
    - Conspiracy
    - Extortion
    -

2.1 Management: For purposes of these procedures, management refers to the President, Vice Presidents, Directors, Managers, Supervisors, or other individuals who manage or supervise funds or other resources, including human resources

3.0 Background

3.1 The Fraud Act 2006 introduced a defined offence of fraud which is broken into three sections

3.1.1 Fraud by false representation - Fraud by false representation is defined by Section 2 of the Act. Representation must be made dishonestly and is made with the intention of making a gain or causing a loss or risk of loss to another. A representation is defined as false if it is untrue or misleading and the person making it knows that it is, or might be, untrue or misleading. Representation can be stated by words or communicated by conduct i.e. written, spoken or by electronic means.

3.1.2 Fraud by failing to disclose information - Fraud by failing to disclose information is defined by Section 3 of the Act, and details that a fraud will have been committed if a person fails to declare information which he/she has a legal duty to disclose. There is a requirement that the person acts dishonestly and intends to make a gain for himself/herself, cause a loss to another or expose another to a risk of loss.

3.1.3 Fraud by abuse of position false representation - Abuse of position. Fraud by abuse of position is defined by Section 4 of the Act and requires a person who is in a privileged position to act dishonestly by abusing the position held; and by doing so, fails to disclose to another person, information which he/she is legally required to disclose. The dishonest act must be with the intention of making a gain for him/her or another. Alternatively, it may be with the intention of causing a loss or risk of loss to another. The offence may be committed by omitting to make a declaration as well as by an act. The Fraud Act 2006 largely replaced the laws relating to obtaining property by deception, obtaining a pecuniary advantage and

other offences that were created under the Theft Act 1978. Whilst the introduction of the Fraud Act 2006 has repealed much of the Theft Act 1978, it does not prevent the prosecution of other offences under the various other Acts, e.g. theft, counterfeiting and falsification of documents

4.0 Reporting Fraud

4.1 Reporting a Suspected Fraud or Incident of Bribery/Corruption, staff should first be familiar and/or read the Whistle-blowing Policy (RGE001) which can be linked with the Anti-Fraud Policy.

4.2 Where it is the wish for the individual to report suspicions they are able to do so by informing RSH and/or a prescribed person anonymously but they may not be able to take the claim further if you have not provided all the information they need. You can give your name but request confidentiality - the person or body you tell should make every effort to protect your identity . However, the organisation will always encourage individuals to come forward and be identified as this is an indication that it is not merely someone with a "grudge" making false accusations and allows the suspicion to be acted upon with greater effectiveness and efficiency.

4.3 RSH and/or the prescribed person will listen to your concern and decide if any action is needed. You may be asked for further information. The claimant must inform the prescribed person and/or organisation immediately if they want to remain anonymous. The claimant will not have a say in how the concern is dealt with. RSH and/or the prescribed person may keep you informed about the action they've taken, but will be unable to provide detail to preserve the integrity of any ongoing investigations.

4.4 The organisation should be responsible for:

- Developing and maintaining effective controls to prevent fraud.
- Carrying out vigorous and prompt investigations if fraud occurs.
- Taking appropriate legal and/or disciplinary action against perpetrators of fraud.
- Taking disciplinary action against supervisors where supervisory failures have contributed to the commission of the fraud.

4.5 Managers should be responsible for:

- Identifying the risks to which systems and procedures are exposed.
- Developing and maintaining effective controls to prevent and detect fraud.
- Ensuring that controls are being complied with.

4.6 Individual members of staff are responsible for:

- Acting with propriety in the use of official resources and in the handling and use of corporate funds whether they are involved with cash or payments systems, receipts or dealing with contractors or suppliers
- Reporting details immediately to (their line manager or next most senior manager) if they suspect that a fraud has been committed or see any suspicious acts or events.

4.7 What to do if you suspect fraud, theft or corruption may be occurring?

4.7.1 Initial action checklist upon discovering a potential fraud:

- Alert the fraud incident manager that an allegation or suspicion exists
- Document date, time and details of initial report/discovery
- Take notes of all observations and actions – if something is worth taking a mental note, it is worth a written note)
- Maintain confidentiality (only inform those people who need to know about the suspected act). Unwarranted disclosure can seriously damage potential successful investigations. Do not confront the suspect.
- Write out in full the suspected act or wrongdoing including:
  - What is alleged to have occurred
  - Who is alleged to have committed the act
  - Is the activity continuing
  - Where did it occur
  - What is the value of the loss or potential loss
  - Who knows of the activity

- Identify all documentary and other evidence connected to the activity
  - Invoices
  - Contracts
  - Purchase orders
  - Cheques
  - Computers
  - Credit card statements etc.

- Obtain evidence and place in a secure area. (only where it is possible without alerting any suspects)
- Protect evidence from damage or contamination
- List each item individually taking note of acquisition (incl. time, date and location) and where the item was securely stored
- Identify all potential witnesses
- Unless electronic evidence is in the process of being destroyed do not go into the suspect/target computer systems
- If possible, secure and/or remove suspect's access to relevant
- computers/systems. Do not allow IT department to examine computer
- Consider other potential suspects and extent of fraud

4.7.2 Convey your concerns to someone with the appropriate authority the responsible person of your particular department, if not those please consult with CEO, CFO, COO or the Chair and report your concerns as soon as possible

4.7.3 Do not approach the concerned individual or be afraid to raise your concerns, don't try to investigate yourself.

4.7.7 Failure to report suspected fraudulent or corrupt activity in a timely manner according to the procedures below will also be subject to disciplinary action.

5.0 What is prohibited?

5.1 In the context of this Policy, fraud is defined as "Conduct that involves deception or dishonesty intended to result in unfair or unlawful gain".

5.2 Fraud may or may not involve a financial gain and when the term is applied to an individual it can include, but is not exhaustive of, the following illustrative examples:

- Forgery or alteration of documents (checks, bank draft, timesheets, invoices, agreements, attendance or flexi time records etc.) or bank accounts belonging to the company or its subsidiaries.
- Misrepresentation of information on documents (expenses, car mileage, petty cash or other employee claim forms).
- Misappropriation of funds, supplies, or assets.
- Theft, disappearance, or destruction of assets.
- Authorising or receiving payments for goods not received or services not performed.
- Authorising or receiving payment for hours not worked.
- Inappropriate use of the company's records and disclosing confidential
- and proprietary information to outside parties
- Using work time to carry out non-work activities
- Using work resources or materials in furthering alternative employment
- e.g. own business interests

6.0 Roles and Responsibilities

6.1 The Management Board is responsible for ensuring the organisation operates:

- To develop an anti-fraud culture and define management and employee responsibilities in this area. To reduce the opportunity for fraud by introducing preventative and detective measures into systems and processes.
- To ensure that anti-fraud controls are considered and built into new systems and processes at the design stage.
- To promote an open and ethical culture within the organisation which deems unethical behaviour unacceptable.
- To increase the vigilance of management and staff through raising fraud risk awareness.
- To ensure that the directors of the group meet their statutory responsibilities towards fraud, as per the requirements for corporate governance.
- To learn from previous incidents and recycle lessons and experiences in fraud prevention and detection globally.
- To encourage management and staff to report their suspicions while guaranteeing anonymity where requested.
- To investigate impartially and thoroughly all cases or suspected cases of fraud, to prosecute offenders and, where appropriate, to seek to recover monies and costs through legal means has relevant policies and systems in place to discourage, detect and report suspected fraudulent activity.
- Maintains appropriate procedures that ensure reported incidents of suspected fraud are promptly and vigorously investigated, and effective sanctions and redress are applied in

instances where fraud is detected.

- The Board is also responsible for ensuring it conducts its own affairs in accordance with the 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.

6.2 Staff Members:

- All staff members are responsible for being vigilant to possible indicators of fraud or attempted fraud, within their respective areas of work.
- Reporting any suspicions of fraud or attempted fraud they encounter.
- Acting with integrity and propriety, within the law, and in accordance with relevant policies, systems and procedures.
- Individuals at all levels of the Organisation will be treated equally regardless of their position, years of service, or affiliation with the company.
- Similarly, staff members should report to their line manager any areas of weakness they identify in procedures or systems; or suggested ways of reducing the possibility of fraud.

6.3 Penalties

Staff found to be involved in fraudulent activity (or theft or corruption) may be subject to one or all the following sanctions.

- Disciplinary - with dismissal usually sought where the offence is considered to constitute "gross misconduct" pursuant to the provisions of the Association Disciplinary Policy.
- Criminal - where the relevant law enforcement agency considers it to be in the public interest to pursue a prosecution.
- Civil - recovery of monies or assets fraudulently or corruptly acquired.
- Professional - disbarring whereby the Council will make a referral to
- the employee's professional regulatory body or bodies where appropriate.

7.0 Monitoring

7.1 As part of its governance systems, the Association maintains various registers to record certain types of activity. Its Fraud, Whistleblowing and Notifiable Events Registers are of relevance to this policy and will be maintained accordingly.

8.0 Anti-Money Laundering

8.1 Why This Applies to RSH

RSH is a Community Interest Company and Registered Provider of Social Housing. It is not a regulated entity under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 and therefore does not carry the full compliance obligations of a bank, solicitor or accountant.

However, the Proceeds of Crime Act 2002 (POCA) applies universally. Any person in any organisation who handles, conceals or fails to report funds they know or suspect to be the proceeds of crime can commit a criminal offence. Given RSH's operating model, which

involves managing agents collecting and remitting rental income, third-party payment flows, and the onboarding of landlords and suppliers, these risks are real and have been evidenced in RSH's own experience.

This section sets out the minimum AML obligations relevant to RSH's size and structure.

8.2 Nominated Officer (MLRO)

RSH shall designate a Nominated Officer, fulfilling the role commonly referred to as a Money Laundering Reporting Officer (MLRO). This role shall be held by the CFO or a senior member of the finance function delegated by the CFO.

8.3 The Nominated Officer is responsible for:

- Receiving all internal suspicious activity reports from staff
- Assessing whether those reports give rise to a suspicion of money laundering
- Deciding whether to make a disclosure to the National Crime Agency (NCA) via the NCA SAR Online Portal
- Maintaining a log of all internal reports received and the outcome of each
- In the absence of the Nominated Officer, the Finance Director shall designate a deputy to cover this function.

8.4 What is Money Laundering?

Money laundering is the process by which the proceeds of criminal activity are made to appear legitimate. Under POCA 2002, the three principal offences are:

- Concealing, disguising, converting or transferring criminal property
- Entering into an arrangement that facilitates another person's acquisition, retention, use or control of criminal property
- Acquiring, using or possessing criminal property

In the context of RSH, the most relevant risk is being drawn into an arrangement where criminal funds pass through RSH's financial structures, whether via managing agent payment flows, landlord transactions, or supplier invoicing.

8.5 Staff Obligation to Report

Any member of staff who knows or suspects that money laundering is occurring must report that suspicion to the Nominated Officer as soon as practicable. The threshold is suspicion, not certainty. If in doubt, report.

8.6 Staff must submit an internal report to the Nominated Officer covering:

- The nature of the suspicious activity
- The person(s) or entity involved
- The value and nature of any funds
- The date and any supporting documentation
- Failure to report a suspicion is itself a criminal offence under Section 330 POCA.

8.7 Tipping Off

Criminal Prohibition – Tipping Off (s.333A POCA)

Once an internal or external report has been made, it is a criminal offence to disclose to the subject of that report — or to anyone else without a clear need to know — that a report has been made or that an investigation may follow.

Staff must NOT inform a managing agent, landlord, supplier or colleague that a suspicious activity report has been filed about them.

Any uncertainty about whether a communication might constitute tipping off must be raised with the Nominated Officer before the communication is made.

The maximum sentence for tipping off is five years' imprisonment.

8.8 Counterparty Due Diligence

RSH already operates a due diligence framework for managing agents, landlords and suppliers under its Contract Management Framework. For AML purposes, the key requirements that must be consistently applied are:

8.8.1 For managing agents and landlords:

- Verify legal identity via Companies House (UK entities) or equivalent — including current registration status, directors and Persons of Significant Control (PSC)
- Confirm the bank account to which RSH will remit funds is held in the entity's own name, evidenced by written confirmation signed by a director
- Any request to change bank account details must be verified directly with a known contact at the entity before acting — not simply by responding to an email or letter
- Where beneficial ownership is unclear or involves offshore structures, escalate to the Nominated Officer before proceeding

8.8.2 For all counterparties:

- Screen against the HM Treasury Consolidated Sanctions List before onboarding and when significant changes occur
- Do not transact with any entity or individual subject to financial sanctions

8.9 Red Flags Specific to RSH's Operations

The following indicators should prompt an internal report to the Nominated Officer:

8.9.1 Managing agents:

- Requests to redirect payments to new or unverified bank accounts, particularly under time pressure
- Use of multiple or frequently changing bank accounts
- Payments from or to third parties not party to the management agreement
- Reluctance to provide identity or ownership documentation

- Companies House records showing dormant, reactivated or struck-off status, or active County Court Judgements
- Undisclosed connected-party relationships between MA directors and RSH officers, landlords or tenants

8.9.2 Landlords and suppliers:

- Beneficial ownership obscured through shell companies or nominees
- Invoice values significantly above or below market rate with no reasonable explanation
- Requests for urgent payment outside standard terms with no supporting documentation
- Changes in ownership or directorship that are not proactively disclosed

8.10 Record Keeping

Consistent with Section 330 POCA and general good governance, RSH shall retain the following for a minimum of five years:

- All internal suspicious activity reports and the Nominated Officer's determination on each
- Any disclosures made to the NCA and the NCA's response
- Due diligence documents collected during counterparty onboarding and review

Records shall be stored securely and made available to the NCA or any other competent authority on lawful request.

8.11 Staff Awareness

All staff with responsibility for managing payments, managing agent relationships, procurement or supplier engagement shall receive awareness briefing on the contents of this section as part of their induction and at each annual policy review. The Finance Director shall confirm completion of this briefing in the annual governance review.

This is not a formal training programme — it is the minimum necessary to ensure staff understand their personal obligations under POCA and know how to make an internal report.

9.0 Review of Policy

9.1 This policy will subject to review every two years by the Finance Department unless changes in legislation require immediate action to be taken. Any changes to the policy will be subject to approval by the Board.

Appendix 1 – Anti-Fraud and Anti-Money Laundering Policy Summary

Policy Summary	
Policy Title	Anti-Fraud and Anti-Money Laundering Policy
Version	v1.3
Policy Reference	RGE002

Policy Owner	Finance Director
Zero Tolerance	RSH operates a zero-tolerance policy towards fraud, corruption and money laundering
AML Legislation	Proceeds of Crime Act 2002 (POCA); Terrorism Act 2000
Nominated Officer (MLRO)	Finance Director or nominated deputy — receives all internal SARs and decides whether to disclose to the NCA
Reporting Threshold	Suspicion is sufficient — staff do not need to be certain before making an internal report
Tipping Off	Criminal offence under s.333A POCA to disclose that a SAR has been made — maximum 5 years' imprisonment
Due Diligence	Applied to managing agents, landlords and suppliers — identity, PSC, bank account verification, sanctions screening
Record Retention	Minimum 5 years for SARs, due diligence documents and NCA disclosures
Staff Awareness	All relevant staff briefed on POCA obligations at induction and annual policy review

Version No.	Changes	Made by	Date
1	None – original version	n/a	September 2023
1.5	Format only	Company Secretary	July 2026