Financial Crime Policy

1. What this policy is about

1.1. This policy:

- Confirms the Board's commitment to maintaining standards of conduct across the Group in an honest and ethical manner, acting professionally, fairly and with integrity in all business dealings and relationships.
- Identifies the scope, nature and type of financial crime risk we are exposed to.
- Defines the principles, culture and expectations in mitigating and managing financial crime risks.
- Identifies and assigns responsibility for mitigating and managing financial crime risks.
- Defines reporting expectations in the event of a suspected or actual financial crime.
- Identifies and assigns responsibility for our response should a financial crime be suspected or crystallise.

2. Our approach

Principles, culture and expectations

2.1. All colleagues are expected to observe the highest standards of integrity. To mitigate the risk of financial crime and to promote and embed this culture, our approach is based on the following principles:

- Selflessness: we operate in the interest of stakeholders.
- Integrity: colleagues avoid placing themselves under any obligation to people or organisations that might try inappropriately to influence or gain favour.
- Accountability: we promote accountability for actions and are open to any necessary scrutiny.
- Openness: we are open and transparent in decision making.
- Honesty: colleagues are truthful in any dealings with our stakeholders.
- Leadership: Members and Executives exhibit these principles and encourage a counter-fraud culture across the organisation.

2.2. To meet its statutory and regulatory obligations and good practice we'll:

- Develop and maintain effective controls to prevent financial crime including training and awareness for all colleagues.
- Undertake regular risk assessments of the likelihood of fraud, corruption and other financial crime arising. Risk assessments are based on relevant good practice, current guidance and analysis of internal and external risk factors.

This policy applies from May 2024
This policy applies to: Livv Housing Group, Livv Homes, Livv Maintenance, First Ark Social Investment

- Establish relevant policies and procedures to mitigate any risks identified.
- Carry out rigorous and prompt investigations if fraud or financial crime occurs.
- Take appropriate legal and/or disciplinary action against perpetrators.
- Take disciplinary action against Board Members, Directors, Managers and Supervisors where their failures have contributed to the commissioning of financial crime.
- Seek to recover any public money, including interest chargeable.
- Report fraud to the Regulator of Social Housing in line with their Fraud Reporting Guidance.
- Provide regular updates to the Audit and Risk Committee.

Financial Crime Risk

2.3. Financial crime can be perpetrated by an internal or external source(s) and can involve major or less significant loss. Crimes can range from organised, co-ordinated, and collusive attacks involving numerous individuals or organised crime groups to lone individuals.

2.4. Financial crime can occur through cyber-attack, exploitation of control weaknesses, disregard to the Group's Policy Framework or abuse of a position of authority.

2.5. Cyber-crime is an umbrella term that describes two closely linked, but distinct ranges of criminal activity. The Government's National Cyber Security Strategy defines these as:

- **Cyber-dependent crimes** - crimes that can be committed only using Information and Communications Technology ('ICT') devices, where the devices are both the tool for committing the crime, and the target of the crime (e.g. developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity).
- **Cyber-enabled crimes** - traditional crimes which can be increased in scale or reach using computers, computer networks or other forms of ICT (e.g. electronic financial fraud, phishing and data theft).

2.6. IT security is covered by the ICT policy and applies to all colleagues. Cyber-attacks can be used to extort money from a company. A hacker might disable services and ask for a "ransom" to restore data. While the method might use IT systems, it is a financial crime.

2.7. Financial crime risk relevant to our activities and operations is detailed below.

Fraud and Theft

2.8. Fraud can occur through false representation, failing to disclose information or by abuse of position. Theft is appropriating property belonging to another with the intention of permanently depriving the other of it.

2.9. Through our activities we are exposed to a range of fraud and theft risks including:

- Asset misappropriation, which involves the theft or misuse of an organisation's assets. Examples include theft of plant, inventory or cash, false invoicing, accounts receivable fraud and payroll fraud.
- Fraudulent statements usually in the form of falsification of financial statements to obtain improper benefit. It also includes falsifying documents such as employee credentials.
- Corruption such as the use of bribes or accepting kickbacks, improper use of confidential information, conflicts of interest and collusive tendering.

Tenancy Fraud

2.10. We are committed to preventing tenancy fraud; this type of fraud can stop applicants in genuine need from accessing housing and could cause us significant and potentially irretrievable financial loss.

2.11. Tenancy fraud can occur in a variety of circumstances and at any stage during the lifetime of a tenancy. This includes the main types of tenancy fraud risk:

- Fraudulently obtaining a social housing tenancy by misrepresentation e.g., providing false identity or misrepresenting personal circumstances.
- Withholding information or making a false statement when applying for a social housing tenancy
- Unlawful subletting, including subletting the whole property or multiple sublets within one property while ceasing to occupy this property.
- Non-occupation by the tenant as their sole or principal home.
- Falsely claimed succession where a tenant dies and someone who is not eligible to succeed to the tenancy retains the property.
- Unauthorised assignment of the tenancy such as an unauthorised mutual exchange or transfer of tenancy without the landlord's permission.
- "Key selling" - where the tenant leaves the property and passes on the keys in return for a one-off lump sum payment or favour.
- Providing misleading information on identity or personal circumstances when purchasing a socially rented home under the Right to Buy or Right to Acquire.

2.12. We are proactive in preventing tenancy fraud, communicating potential risks, and defining and implementing controls to prevent and detect tenancy fraud. This approach is consistent with Consumer Regulations. The Tenancy Policy is also part of the approach to tenancy fraud and should be reviewed when considering tenancy fraud.

Bribery and Corruption

2.13. Bribery can be the offering, promising or giving of a bribe, and the requesting, agreeing to receive or accepting of a bribe. It also includes the offence of the failure of commercial organisations to prevent bribery.

2.14. We take a risk-based approach to managing bribery risks and periodically assess the nature and extent of our exposure to external and internal risks of bribery aligned to the Ministry of Justice Bribery Act Guidance. Our internal control framework enables proportionate safeguards and controls to protect against bribery risks.

2.15. Corruption is an abuse of a position of trust to gain an undue advantage.

2.16. All offers of gifts or hospitality made or received, even if they are not accepted, should be declared using the Hospitality and Gifts Declaration. Further information on accepting or refusing offers of gifts and hospitality can be found in the Probity and Expenses Policy.

Facilitation of Tax Evasion

2.17. The corporate offence relates to who may be held to account for crimes relating to tax evasion whether the tax evaded is owed in the UK or in a foreign country. It includes the offence of failing to prevent an associated person criminally facilitating the evasion of a tax.

2.18. We adopt a risk-based approach to inform reasonable prevention procedure requirements. This aligns to the nature and extent of our exposure to facilitation of tax evasion and Tackling tax evasion: Government guidance for the corporate offences of failure to prevent the criminal facilitation of tax evasion. Our internal control framework enables proportionate safeguards and controls to protect against facilitation of tax evasion risks.

Money Laundering

2.19. This is where money gained from the proceeds of crime is put through a process to make it appear to be from legitimate sources of income.

2.20. The Group is not a regulated body under the terms of the Money Laundering Regulations however we remain vigilant against the offence occurring and have reasonable measures in place to mitigate this risk. Measures include risk assessment to inform source of funds confirmation controls and training and communication to support colleagues to remain alert for suspicious transactions.

2.21. Examples of money laundering might include someone who wants to deal with large amounts of cash, or someone who wants to engage in a transaction which is outside the scope of their normal business.

Responding to incidents

2.22. The Group does not tolerate financial crime in any form. Where relevant we will pursue prosecution for criminal acts. This will be a proportionate response that considers the presenting circumstances.

2.23. To report financial crime, review the Financial Crime Process.

3. Responsibilities

3.1 All colleagues are responsible for carrying out their work in line with this policy and associated procedures. The Director of Risk, Audit & Assurance is responsible for overall implementation of this policy. Specific responsibilities are set out below:

Role	Responsibility
Common Board	Board members are required to operate within: • The legal, regulatory and statutory framework • Standing Orders and Financial Regulations • The Group's Board Member Code of Conduct • The Group's Non-Executive Director's Probity Policy The Board is responsible for leading and promoting an anti-fraud culture.
Audit & Risk Committee (ARC)	Approve of the Financial Crime Policy and oversight, monitoring and review of incidents and the Fraud Register.
Chief Executive and Executive Directors	Establish and maintain a sound system of internal control. This includes in consideration to mitigating and managing the prevention of financial crime wherever possible.
Executive Director – Finance, Risk and Performance	Oversight of the risk of fraud and financial crime rests with the EDFRP. Responsibilities include: • Promote an anti-fraud culture. • Appropriate risk management (see also the Risk Management Strategy, Policy and Guidelines). • Agree relevant fraud and financial crime investigations where a suspected or actual fraud or financial crime is evident.
Director of Risk, Audit & Assurance	• Develop, maintain and promote the Financial Crime Policy. • Undertake risk assessment activity relevant to the financial crime risks the organisation is exposed to. • Support Directors and Heads of Service in control and assurance activity including fraud prevention and detection measures. • Arrange relevant fraud and financial crime investigation in liaison with the EDFRP

Role	Responsibility
Director of Finance and Investment	• Complete the Fraud report and return to NROSH in a timely manner. • Maintain and promote adequate controls and oversight over the financial management of the Group. • Liaise with the EDFRP and Director of Risk, Audit & Assurance where necessary in matters of fraud and financial crime.
Internal Audit	Independent assurance on the adequacy and effectiveness of key controls including fraud and financial controls where relevant, through the completion of the Internal Audit Plan.
Directors	• Ensure that an adequate system of internal control exists within their areas of responsibility and that controls operate effectively. • Prevent and detect fraud and financial crime. • Assess the types of risk involved in the operations for which they are responsible. • Review and regularly test control systems for which they are responsible. • Ensure that controls are complied with and their systems continue to operate effectively. • Implement new controls to reduce the risk of similar fraud occurring where frauds have taken place. • Incorporate anti-fraud controls in all systems at the design phase.
All colleagues	• Understand and comply with the Employee Code of Conduct and demonstrate due regularity and propriety in the use of official resources and the handling and use of funds whether they are involved with cash or payments systems, receipts or dealing with suppliers. • Be alert to the possibility of fraud; and taking special care where unusual events or transactions occur. • Report details immediately through the appropriate channel if they suspect that a fraud, act of bribery, money laundering or other financial crime has been committed or see any suspicious acts or events. • Cooperate fully with whoever is conducting internal checks, reviews or investigations.
Risk and Assurance team	Facilitate the consistent application of this policy.

4. Monitoring and review

4.1. Financial crime risk is reviewed and assessed on at least an annual basis unless changes in the regulatory or risk environment require more frequent review.

4.2. Suspected or actual incidents of financial crime are reported in line with the Financial Crime Escalation Protocol (see Appendix A) and notified to the Director Finance and Investment.

4.3. We maintain a Fraud Register, recording suspected or actual incidents of fraud or financial crime. The Audit and Risk Committee review the Fraud Register and Incidents along with planned actions, at each meeting. Major and catastrophic rated incidents are escalated to Board along with review and approval of planned actions.

4.4. The Group also maintains a register of gifts and hospitality which is reviewed by the Audit and Risk Committee at each meeting.

4.5. We will review this policy every three years, or sooner if our monitoring of the policy identifies that changes are required, for example because of changes to law, regulation or related Livv strategies and policies.

Control framework

Compliance

This policy supports compliance with:

- Fraud (as defined in the Fraud Act 2006 and Prevention of Social Housing Fraud Act 2013)
- Theft (as defined in the Theft Act (1968 and 1978))
- Bribery (as defined in the Bribery Act 2010)
- Facilitation of tax evasion (as defined in the Criminal Finances Act 2017)
- Money Laundering (as defined in the Proceeds of Crime Act 2002 Part 7 - Money Laundering Offences)
- Economic Crime and Corporate Transparency Act 2023
- Consumer Regulation – Tenancy Standard

Document control	
Version	1.0
Policy applies from	7 May 2024
Policy applies to	All Livv Housing Group organisations
Approved by	Audit and Risk Committee
Approved on	7 May 2024
Replacing	Financial Crime Policy 2021-24
Next review due by	May 2027
Responsible Executive Director	Executive Director - Finance, Risk and Performance
Policy author	Director – Risk, Audit and Assurance
Equality Analysis	January 2024
Environmental Impact Assessment	N/A
Circulation	Intranet, website

Version control		
Version	**Date of Review**	**Summary of changes made**
1.0	May 2024	Full policy review Included money laundering references Reviewed Economic Crime and Corporate Transparency Act requirements

Appendix A: Escalation Protocol