

Financial Crime Prevention Policy and Procedures

Procedure ref: Compliance

Procedure author/holder: Director of Governance & Compliance

Date approved: 2 August 2018

Approved by: Board

Effective date: 2 August 2018

Review date: August 2021

1. Scope

- 1.1 Our Financial Crime Prevention Policy and procedures apply to the following in their business conduct with us: all employees at all levels, agency workers, seconded workers, apprentices, Board and Committee Members, residents, volunteers, contractors, external consultants, third-party representatives and joint venture partners with or with whom we collaborate on projects, or any other person associated with us, wherever located.

Breach of policy or procedures

- 1.2 You are expected to read, understand and comply with this policy and the procedures for tackling financial crime. The procedures are designed to help you to avoid any suggestion of influence by biased or improper motives.
- 1.3 LiveWest will take action against you if you perpetrate or attempt to perpetrate a financial crime, and against any person whose conduct allows such activity to be committed. This includes a deliberate failure to speak up when there was clear evidence of corruption by others. If you are in a management role and fail to report such incidents you may be deemed to have "consented to connive" in the activity and you could be prosecuted for the offence.
- 1.4 Any employee who breaches this policy will face disciplinary action, which could result in dismissal for misconduct or gross misconduct.
- 1.5 If you are a Board or Committee Member and you breach this policy your service agreement will be terminated.
- 1.6 We may terminate our relationship with other individuals and organisations working on our behalf if they breach this policy.
-

- 1.7 Suspected criminal activity may be reported to the police or other external agencies for investigation, which may lead to a prosecution.

2 Policy statement

- 2.1 We will act professionally, fairly, honestly, and with integrity in all our business dealings and relationships.
- 2.2 We will not tolerate any form of fraud, bribery, money laundering, the criminal facilitation of tax evasion or other dishonest behaviour (collectively referred to here as “financial crime”).
- 2.3 We will uphold all laws relevant to countering financial crime including the Bribery Act 2010, the Fraud Act 2006, the Proceeds of Crime Act 2002, the Money Laundering, Terrorist Financing and Transfer of Funds (information on the Payer) Regulations 2017 and the Criminal Finances Act 2017.
- 2.4 We will not be party to any transaction where there is a reasonable ground to believe or suspect that the other party is using the proceeds of crime as consideration or payment for the transaction. The grounds for suspicion do not have to be clear or firmly grounded and targeted on specific facts but the suspicion must be something more than merely fanciful.
- 2.5 We will not accept cash payments in excess of £2,000, without the approval of an Executive Director and reported to the Money Laundering Reporting Officer.
- 2.6 We are committed to protecting LiveWest’s resources from financial crime and will provide awareness training for our employees, Board and Committee Members, as appropriate.
- 2.7 We will take proportionate action to recover any money or property that has been lost.
- 2.8 We will co-operate with the police and other external agencies in any investigations concerning financial crime or other corrupt activity.
- 2.9 We encourage our employees, Board and Committee Members to use LiveWest’s confidential reporting (whistleblowing) procedures, without fear of reprisal, to raise any concerns they may have about financial crime or corrupt activity affecting LiveWest or its resources.

- 2.10 We will review this policy and associated procedures at least every three years or more frequently if required by changes in regulation or legislation or if our operating environment changes substantially.

3 Purpose and anticipated outcomes of this Policy

- 3.1 The purpose of this document is three-fold:
- To provide information and guidance to help you to recognise and avoid financial crime in its many forms.
 - To set out our approach to tackling the risk of financial crime, including prevention and detection.
 - To help you to understand your responsibilities in observing and upholding our position on preventing financial crime.

4 Fraud

- 4.1 The Fraud Act 2006 created a criminal offence of fraud and defines three ways of committing such an offence:
- Fraud by false representation i.e. dishonestly making an untrue or misleading representation. This could be made verbally, in writing or by electronic means.
 - Fraud by failing to disclose information i.e. dishonestly failing to disclose information to another person, where there is a legal duty to do so.
 - Fraud by abuse of position i.e. where a person occupies a position in which they are expected to safeguard, or not to act against, the financial interests of another person, and they dishonestly abuse that position.

The term "person" includes an organisation.

- 4.2 For fraud to occur the offender's conduct must be dishonest and their intention must be to make a gain, or cause a loss (or the risk of a loss) to another.
- 4.3 Fraud carries a maximum sentence of 10 years' imprisonment.

5 Bribery

- 5.1 Bribery is generally defined as offering or giving, requesting or receiving gifts, money, hospitality or other favours in return for providing something of value to the briber. From this general definition, it should be noted that:
- A bribe does not need to be money. It can be any form of advantage, for example an award of a contract, lavish hospitality or gifts, or an offer of employment.
 - A recipient of a bribe does not need to benefit personally.
 - Actual payment of a bribe does not need to occur for there to be a criminal offence; offering or requesting a payment (or some other favour) can amount to bribery in itself. The recipient does not necessarily need to do anything in return for the offence to occur.
- 5.2 We have identified that the following activities or areas of operation within LiveWest could be particularly vulnerable to the risk of bribery:
- Procurement and the supply chain;
 - Sales or purchases of land, residential property or commercial property;
- 5.3 The Bribery Act 2010 reformed the criminal law of bribery, making it clearer and easier to tackle this offence and prosecute. It introduced a corporate offence of failing to prevent bribery by “associated persons”. These are persons providing services for us or on our behalf and include employees, agents, subcontractors, joint venture partners etc.
- 5.4 Penalties for individual offenders under the Bribery Act are severe and include up to 10 years’ imprisonment and an unlimited fine. LiveWest or its subsidiary companies face an unlimited fine if we fail to prevent bribery and do not have “adequate procedures” to do so.
- 5.5 If you are a senior manager and you are found to have “consented or connived” in bribery by others you will be equally liable for the offence under the Bribery Act.

6 Money Laundering

- 6.1 Money laundering is the process by which money or other assets that were obtained criminally (Criminal Property) are exchanged for 'clean' money or assets with no obvious link to their criminal origins. It also covers money which is used to fund terrorism. The offences relating to money laundering are set out in the Proceeds of Crime Act 2002 ("POCA") and Money Laundering, Terrorist Financing and Transfer of Funds (information on the Payer) Regulations 2017.
- 6.2 An offence may be committed if we are party to transactions where we know or suspect Criminal Property forms part of the transaction.
- 6.3 Money laundering most commonly occurs by means of cash transactions but can also occur through the use of bank payments whether by cheque, debit card or direct banking payment.
- 6.4 We have identified that the following areas of operation within LiveWest could be particularly vulnerable to attempts at money laundering:
- sales or purchases of land, residential property or commercial property, whether outright or initial shared ownership that have been acquired from the proceeds of crime;
 - borrowing and repayment of money.
- 6.5 The Penalties for individual offenders under the POCA for money laundering are severe and include up to 14 years' imprisonment.

7 Tax evasion facilitation

- 7.2 For the purposes of this policy tax evasion means the offence of cheating the public revenue or fraudulently evading UK tax, and is a criminal offence.
- 7.3 Tax evasion facilitation also means being knowingly concerned in or taking steps with a view to, the fraudulent evasion of tax by another person, or aiding, abetting, counselling or procuring the commission of that offence.
- 7.4 Tax evasion facilitation is a criminal offence, where it is done deliberately and dishonestly.
- 7.5 A deliberate failure to report suspected tax evasion or "turning a blind eye" to suspicious activity could also amount to criminal facilitation of tax evasion.
- 7.6 Under the Criminal Finances Act 2017, a separate criminal offence is automatically committed by a corporate entity or partnership where the tax evasion is facilitated by a person acting in the capacity of an "associated person" to that body. For the offence to be made out, the associated person
-

must deliberately and dishonestly take action to facilitate the tax evasion by the taxpayer. If the associated person accidentally, ignorantly, or negligently facilitates the tax evasion, then the corporate offence will not have been committed. This means that LiveWest does not have to have deliberately or dishonestly facilitated the tax evasion itself; the fact that the associated person has done so creates the liability for LiveWest.

- 7.7 Tax evasion is not the same as tax avoidance or tax planning. Tax evasion involves deliberate and dishonest conduct. Tax avoidance is not illegal and involves taking steps, within the law, to minimise tax payable (or maximise tax reliefs).
- 7.8 Within LiveWest we have identified that following areas of operation could be more vulnerable to attempts by associated persons to facilitate criminal tax evasion:
- Human resources and payroll;
 - The supply chain;
 - Sales and purchases of land, residential property or commercial property.
- 7.9 As an employer, if we fail to prevent our employees, workers, agents or service providers facilitating tax evasion, we can face criminal sanctions including an unlimited fine, as well as significant damage to our reputation.

8 Prevention of financial crime

- 8.2 The likelihood of financial crime occurring can be reduced, to an extent, by the use of preventative controls and the operation of an appropriate culture within LiveWest, for example through our values.
- 8.3 The impact of financial crime occurring measured in monetary, resident/customer, or reputational, terms, can be reduced if you are aware of the risks, if we have appropriate internal controls to detect any irregular or corrupt activity and an effective response plan is in place.
- 8.4 We have in place a framework of preventative measures, including internal controls, designed to prevent financial crime occurring in the first instance.
- These consist of rules, regulations, policies and procedures within which you are expected to operate and include:

- Our Code of Conduct and Probity Standards.
- Our Confidential Reporting (Whistleblowing) policy.
- Our Treasury Policy.
- Disciplinary and Grievance Policies for employees.
- Our internal financial regulations, including procurement procedures.
- Our sales procedures, including customer due diligence and due diligence on the other party to the transaction which may be a seller or buyer. The level of due diligence undertaken depending on our risk assessment of each person.
- Standing Orders for boards and committees, including delegated authorities.
- Register of Interests of employees, Board and Committee Members.
- Registers of Gifts and Hospitality received and declined.
- Your contract of employment if you are an employee
- Your service agreement if you are a Board or Committee Member.

Cyber crime

- 8.5 In addition, we carry out a regular IT security test for LiveWest's network infrastructure. The objective of the security review being to assess the security in place over our network infrastructure and reduce the possibility of cyber crime.
- 8.6 We also have a public website which provides information about LiveWest. The website is considered to be informational in that it does not provide any login or registration services. The website is externally hosted by a third party service provider. As a result, the risk of vulnerability on the website affecting our internal systems is considerably reduced.

Acceptance of cash payments

- 8.7 We will not accept cash payments in excess of £2,000, whether for one transaction or cumulatively for a series of transactions, without the approval of an Executive Director and reported to the Money Laundering Reporting Officer (see section 10.5 below).

Foreign currency

- 8.8 For borrowing of money or purchase of foreign currency, the counterparty must be a well-known financial institution regulated in the UK by the Financial Control Authority (Treasury Policy section 10).

9 Detection of financial crime

- 9.2 In addition to internal controls, employee awareness of financial crime is a key element of our approach to detection. Fraud and bribery training is mandatory for new employees, Board and Committee Members and will be refreshed on a regular basis, at least every three years.

Training on money laundering and tax evasion will be mandatory for employees working in those areas deemed to be vulnerable to these risks.

- 9.3 You should be vigilant to the warning signs and indicators of financial crime, some examples of which can be found in Appendix 1.
- 9.4 If you are a director or a manager, you should be particularly alert to factors which may indicate that financial crime is, or could be, taking place e.g. excessive expenses claims, frequent hospitality with a particular supplier.
- 9.5 Suspected financial crime may also be detected by the audit process or by a report from a third party outside LiveWest using the confidential fraud reporting mailbox on our website.

10 Responsibility for prevention and detection

- 10.2 You are responsible for acting openly and honestly in how you use LiveWest's assets and incur liabilities, in how you deal with colleagues, residents, contractors and suppliers, and for reporting immediately if you suspect an attempted or actual financial crime has taken place.
- 10.3 The LiveWest Board is accountable for ensuring that adequate systems of internal control are operated within the LiveWest group. Responsibility for ensuring that adequate systems of internal financial control are operated within LiveWest has been delegated by means of our internal financial regulations to the Executive

Director of Finance. Responsibility for operating wider internal controls is delegated to the Executive Team (“ET”).

- 10.4 If you are a director or manager it is your responsibility to actively deter, prevent, and detect financial crime by maintaining good control systems and ensuring that your colleagues are familiar with them. This includes identifying the risks to which your business activities are exposed, implementing effective systems of internal control to prevent and detect financial crime, and ensuring that these controls operate effectively.
- 10.5 Internal audit supports the LiveWest Board and ET in fulfilling their internal control responsibilities by testing and evaluating the appropriateness and effectiveness of controls in relation to the risks to which LiveWest is exposed. The internal audit reports are subject to scrutiny by the Audit & Risk Committee, as well as our Register of Gifts and Hospitality, and our Register of fraudulent activity, in order to provide assurance to the LiveWest Board.

Money Laundering Reporting Officer

- 10.6 Under the Money Laundering, Terrorist Financing and Transfer of Funds (information on the Payer) Regulations 2017, we are required to designate a Money Laundering Reporting Officer (“MLRO”).
- 10.7 Our MLRO is our Company Secretary and is responsible for ensuring compliance with the relevant requirements of the money laundering legislation and dealing with any queries about it. They can be contacted by email at Report.Fraud@livewest.co.uk

11 Notifying us of an actual or suspected financial crime

- 11.2 LiveWest’s confidential reporting procedures are set out in our Confidential Reporting (Whistleblowing) Policy (2018) which can be found in the Policy & Procedures Library” which is part of The Resource Hub on OurSpace
 - 11.3 If you suspect or detect a financial crime you must immediately notify your line manager or a more senior manager as appropriate.
 - 11.4 If for some reason it is not possible to speak with your line manager or you are not an employee, and/or you are in any doubt about whether or how to report your concern, you should contact our Company Secretary, who is the person responsible for ensuring that our Confidential Reporting (Whistleblowing) Policy and Procedures operate effectively and advising on or investigating issues
-

raised. They can be contacted by email in the first instance at Report.Fraud@livewest.co.uk

- 11.5 If you are unsure about whether a particular act constitutes financial crime or other corrupt activity, raise it with your line manager or seek guidance from the Executive Director of Finance, or the Director of Governance & Compliance, as soon as possible.
- 11.6 You should not tell or inform the person involved in the suspected financial crime that a suspicion has been raised or that details of a transaction have or may be reported to an external regulator (such as the National Crime Agency), or that law enforcement agencies may investigate the matter. To do so may be regarded as "tipping of" which is a criminal offence

12 Reporting externally

Housing benefit fraud

- 12.2 Potential housing benefit fraud will be reported to both the Department for Work and Pensions and/or the local authority.

Housing regulator

- 12.3 Any suspected fraud in excess of £5,000 (or any other limit agreed with the Regulator of Social Housing "RSH") or equivalent in value, or any suspected fraud perpetrated or attempted by a Board or Committee Member or ET director, no matter how low its value, will be reported to the RSH by the Chief Executive or the Deputy Chief Executive or the Company Secretary or the Chair of the Audit & Risk Committee or the Group Chair, as appropriate, immediately upon discovery.
- 12.4 A report on any losses from fraudulent activity will be reported annually to the RSH as required under its governance standard.

Reporting to the National Crime Agency ("NCA")

- 12.5 The MLRO in consultation with Chief Executive will decide whether the suspicion warrants reporting to the NCA in the form of a suspicious activity report concerning money laundering ("SAR").
- 12.6 The MLRO must make a report to the NCA as soon as it is practical to do so, even if no transaction takes place, if they consider that there is knowledge, suspicion or reasonable grounds for knowledge or suspicion that another person is engaged in money laundering or has or has attempted to finance terrorism.

- 12.7 If a SAR is made after the transaction has completed, we are permitted to continue to do business with the customer. However, you should not enter into a new transaction until consent has been received from our MLRO to do so.
- 12.8 If a SAR is made before a transaction is completed or at the start of a business relationship, the MLRO must ask for consent to go ahead with that particular transaction. We cannot ask for general consent to trade with that person. We cannot proceed with the transaction until the MLRO has received consent from the NCA.
- 12.9 If the MLRO makes a report to the NCA and the NCA give consent to proceed, the transaction can be completed without any risk of committing a proceeds of crime offence.
- 12.10 All SARs must be reported to the Group Chair or the Chair of the Audit & Risk Committee.

13 Internal records of notifications

- 13.2 A record of every suspicion of financial crime notified internally at stage 1 or above shall be entered on our Fraud Register.
- 13.3 The register will be maintained by the Company Secretary or their delegate and for data protection purposes the entries will be kept anonymous.
- 13.4 If you are an ET director, or your line manager is an ET director, you are required to notify the Company Secretary or their delegate immediately, and each quarter, of any actual or suspected financial crime reported in your areas of responsibility. Such activity will be recorded in the Fraud Register and action taken as necessary.
- 13.5 The Fraud Register will be open to inspection by the RSH at any time and will be reviewed by the Audit & Risk Committee on a regular basis.

14 Review

- 14.2 This policy and associated procedures will be reviewed at least every three years or more frequently if required by changes in regulation or legislation or if our operating environment changes substantially.

14.3 In addition, the effectiveness of the policy and procedures will be reviewed immediately following a significant¹ incident.

¹ Significant means any act of fraud , bribery, money laundering , tax evasion facilitation or other corrupt activity which would need to be reported to the housing regulator (see section 12.2 – reporting externally).