Anti-Money Laundering Policy

1.0 SCOPE

Purpose

1.1. This document sets out whg's Policy towards limiting our exposure to money laundering. whg values its reputation for ethical behaviour and for financial probity and reliability. It recognises that as well as the commission of any crime, any involvement in money laundering will also reflect adversely on its image and reputation.

1.2. Money laundering is the process of moving illegally acquired cash through financial systems so that it appears to have come from a legitimate source. Criminals try to conceal the origin and true ownership of the proceeds of their activities using various means to feed it back into the financial system after a transaction or series of transactions designed to disguise the original source of the funds. Money laundering also covers money, however come by, which is used to fund terrorism.

1.3. 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.

1.4. An offence could be committed by any colleague simply by accepting cash from someone in the knowledge that the cash is from the proceeds of crime.

Legal and regulatory framework

1.5. The Regulator of Social Housing's Governance and Financial Viability Standard requires all registered providers to adhere to all relevant law.

1.6. Registered Providers shall manage their resources effectively to ensure their viability is maintained while ensuring that social housing assets are not put at undue risk

1.7. The legislation relevant to the Policy are:

- Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017;
- Estate Agents Act 1979;
- Terrorism Act 2000;
- Proceeds of Crime Act 2002;
- Protecting the Public Purse 2014
- The Criminal Finances Act 2017
- The Money Laundering and Transfer of Funds (Information) (Amendment) (EU Exit) Regulations 2019

1.8. Money Laundering Offences

1.8.1. Under the Proceeds of Crime Act 2002 (POCA) money laundering offences are committed when a person:

- Conceals criminal property (POCA, section 327);
- Enters into an arrangement regarding criminal property (POCA, section 328);
- Acquires, uses or possesses criminal property (POCA section 329).

These are serious offences that carry a maximum 14 year sentence.

1.8.2. In addition there are two 'Third Party' offences where there is a risk they may be committed by colleagues:

- Failure to disclose one of the principal offences; and
- Tipping Off – where someone informs a person suspected of money laundering in such a way as to reduce the likelihood of their being investigated.

2.0 POLICY STATEMENT

2.1. whg will not accept any level of money laundering, irregularity or corruption; any case will be thoroughly investigated and dealt with appropriately. Colleagues have a responsibility to make every effort to minimise the risk to whg's assets and interests from money laundering, irregularity and corruption.

2.2. This Policy sets out the risk to whg and to colleagues associated with money laundering, the procedures in place to prevent offences being committed relating to money laundering and the procedures to be followed if colleagues identify or suspect that money laundering is attempted.

2.3. Arrangements to comply with legislation and regulations

2.3.1. To ensure compliance with the legislation and regulations relating to money laundering whg will:

- Put in place checks, controls and procedures in order to anticipate and prevent money laundering or terrorist financing;
- Have in place proper identifying, recording and reporting procedures;
- Make colleagues aware of the Money Laundering Regulations 2017, the Terrorism Act 2000 and the Proceeds of Crime Act 2002 and the procedures for reporting suspicions or activity relating to money laundering;
- Confirm the identity of a customer before entering into a business relationship or occasional transaction with him/her and obtaining information on the purpose or nature of the business relationship;
- Conduct ongoing monitoring of the business relationship as appropriate to ensure the business transactions are consistent with our knowledge of the customer and the customers business;
- Keep records obtained in establishing our customers' identity and of business relationships for at least five years from the transaction or when the business relationship ends;
- Provide clear guidance to colleagues on the Policy and arrangements for accepting cash and any checks that should be carried out when cash is offered as a payment or part payment for any transaction;
- Provide adequate training for colleagues in procedures and law relating to money laundering and terrorist financing;
- Appoint a Money Laundering Reporting Officer (MLRO).

2.4. Estate agency activity

2.4.1. An area where whg may be susceptible to money laundering is in relation to Shared Ownership activity. whg will comply with HMRC regulation relating to estate agency activity, which requires us to register with them if we advertise a property for sale in which we have a joint interest with a customer such as a shared ownership property or if we instruct an estate agent or lawyer to advertise such a property for sale.

2.5. Money Laundering Reporting Officer

2.5.1. All suspicious activity must be reported immediately to the MLRO. The MLRO is responsible for:

- Reporting suspicious activity to the National Crime Agency;
- Ensuring that any suspicious activities are recorded in a specific register;
- Ensuring that colleagues are appropriately trained.

2.6. Roles and responsibilities

2.6.1. All colleagues and Board Members are expected to comply with the arrangements set out in this Policy.

2.7. Detailed procedures, possible signs of money laundering, risk assessment

requirements and due diligence

2.7.1. Possible signs of money laundering, procedures for reporting and recording, risk assessment requirements and due diligence requirements are included in Appendices:

- Appendix 1 - examples of money laundering and possible signs of money laundering;
- Appendix 2 - reporting and record keeping procedures;
- Appendix 3 - risk assessment requirements;
- Appendix 4 - sets out the due diligence requirements.

3.0 PERFORMANCE MEASURES

3.1. We will monitor our performance in relation to:

- Provision of training for colleagues to ensure they understand their role and responsibility in relation to this Policy;
- Recording any suspicious activity;
- Reporting suspicions to National Crime Agency.

4.0 MONITOR AND REVIEW

4.1. The Board has delegated to the Audit and Assurance Committee (AAC) responsibility for reviewing and approving this Policy.

4.2. This Policy will be monitored by the Corporate Director of Governance and Compliance and reviewed every three years, or sooner in the event of significant legal or regulatory developments, by the AAC.

4.3. Adherence to the Policy will be included in the annual review of internal controls reported to the Audit and Assurance Committee.

5.0 ASSOCIATED DOCUMENTS, POLICIES AND PROCEDURES

5.1. Documents, policies and procedures associated with this Policy are:

- Money Laundering Regulations 2017
- EC Third Money Laundering Directive in the UK.
- Estate Agents Act 1979
- Terrorism Act 2000
- Proceeds of Crime Act 2002
- whg Code of Conduct
- Whistleblowing Policy
- Fraud Prevention Policy
- Protecting the Public Purse 2014
- The Criminal Finances Act 2017
- The Money Laundering and Transfer of Funds Regulations 2019

Appendices

Appendix 1: Examples Of Money Laundering

Appendix 2: Reporting And Record Keeping

Appendix 3: Risk Assessment

Appendix 4: Due Diligence

APPENDIX 1

EXAMPLES OF MONEY LAUNDERING

One example of money laundering that may be relevant to the social housing sector is in relation to property sales, including Right to Buy transactions, Shared Ownership and homes sold for outright sale. To protect whg we would usually expect the payment to go through a solicitor or mortgage company.

The following situations may indicate that a customer or transaction is suspect:

- Checking a new customer's identity is difficult
- Reluctance from a new customer to provide details of their identity
- The size of the transaction is not consistent with previous activity. For example, a customer on housing benefit or other benefits suddenly has the funds for a deposit to fund a house purchase
- The financial circumstances of an existing customer have changed dramatically
- Money is paid by a third party who has no obvious link with the transaction. Money launderers often use front buyers to enter into transactions on their behalf. The money for a deposit or even to pay a mortgage may have come from someone other than the customer and could very well be the proceeds of crime
- A customer wants to pay a large sum in cash
- A customer applies pressure to accept his or her business before the necessary checks are carried out
- A customer makes an approach to purchase a property then backs off on realising his or her identity will be checked for money laundering purposes.

The misuse of properties for criminal purposes

- Cannabis farms in properties can be a danger to other residents due to an increased fire risk. Colleagues should be trained in recognising the tell-tale signs of cannabis cultivation.
- Human trafficking and exploitation of women and children is the modern day slave trade and a fast growing area of criminality. Properties are used as brothels and accommodation for the victims of trafficking.
- Tenancy fraud and sub-letting has resulted in thousands of properties being unavailable for social housing.
- Drug trafficking and illicit laboratories with the related problems of anti-social behaviour and danger to residents.

Fraud (internal and external)

Fraud, whether perpetrated by employees or from another source, creates the proceeds of crime which are then laundered. Housing associations are susceptible to the same risks as any business. Some examples are:

- Collusion fraud by contractors or suppliers to corrupt the tendering process or colleagues involved in such collusion
- Gratuities or incentives to colleagues to influence the award of contracts
- Criminals setting up front companies or shell companies to defraud associations
- Foreign lenders which are fronts for criminality posing as bona fide financial institutions to lend money to associations.

APPENDIX 2

REPORTING AND RECORD KEEPING

Colleagues must report suspicions or actual money laundering to the Money Laundering Reporting Officer (MLRO) who is currently the Corporate Director of Governance and Compliance, as soon as practicable when they know or suspect, or have reasonable grounds for knowing or suspecting, that a person is engaged in money laundering or terrorist financing. Failing to report such knowledge or suspicion is a criminal offence (see section 4 of the Act).

After consideration of the contents of an internal report, the MLRO may decide to report the matter to the National Crime Agency. Details of how to report such matters are available on the National Crime Agency's website
http://www.nationalcrimeagency.gov.uk/

Reports of suspicious activity, both internal and external must be treated as confidential and securely stored. There are offences of tipping off and prejudicing an investigation which carries severe penalties connected with unlawful disclosure of information following a report having been made.

Where it is decided not to report to the National Crime Agency the MLRO should fully document the rationale behind any such decisions and retain those records.

APPENDIX 3

RISK ASSESSMENT

- whg will regularly conduct risk assessments to determine which areas of activity within the Group are most at risk of being exposed to money laundering, taking action where required to manage those risks identified.
- whg will monitor the adequacy of procedures in place to ensure that they enable adequate monitoring of those teams, contracts and transactions which are considered most at risk. This will include identifying any new types of business or with customers who are new to whg.

There is no requirement for risk assessment to be a complicated process but the system should be capable of demonstrating that it is effective and addresses the identified risk factors. Decisions taken in respect of initial or ongoing risk assessment should also be documented and retained. whg will need to look at the risks which apply to our individual business models and take appropriate protective measures.

Internal controls

The core obligations in respect of internal controls are that whg must establish and maintain adequate and appropriate policies and procedures to forestall and prevent money laundering. These controls must take account of the risk factors which the business faces; and where activities are outsourced the business should ensure that outsourcing does not result in reduced standards. An example of this would be where client identification procedures are outsourced to another agency in relation to Shared Ownership schemes.

APPENDIX 4

DUE DILIGENCE

Customer due diligence measures and ongoing monitoring

One of the most effective methods for protecting a business against attack by money launderers is to carry out stringent checks on the identity of customers and to know who the beneficial owner in any transaction is.

What is customer due diligence?
Steps to identify a customer and the level of verification needed will differ dependent on the nature of the transaction, the client, and the perceived risk of money laundering or terrorist financing.

The basic first step is identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source. In many cases, where the risk is assessed to be low, this may be all that is needed to be satisfied that enough is known about the customer to engage in a transaction.

It is, however, important to be aware that there are many forged and stolen documents in circulation, such as driving licences, passports and utility invoices, and it may be advisable to use electronic methods of customer identification – whg will look at the risks which apply to our business models and implement appropriate protective measures. It is necessary to ensure that any system used meets the requirements in relation to the depth, breadth and quality of data.

When electronic evidence of identity is sought, it will not be necessary to ask the customer's permission to perform a check but the customer must be informed that the check is being done. It may be useful to include mention that this may be necessary in documentation sent to customers along the following lines '…whg is legally bound to comply with the Money Laundering Regulations 2007, the Proceeds of Crime Act 2002 and the UK Terrorism Acts. We may therefore utilise electronic means of verifying customers' identity…'

Enhanced due diligence

In some circumstances, it may be necessary to carry out further due diligence on a risk-based approach where the standard evidence of identification is not sufficient for example:

Where the customer has not been physically present for identification, that is non face-to-face customers: whg will take account of the increased risk by doing one or more of the following:

- Obtaining additional information or evidence to establish the customer's identity
- Undertaking additional measures to verify the documents supplied or requiring certification by a financial or credit institution
- Ensuring that the first payment of the operation is carried out through an account with a credit institution in the customer's name.

- Where the customer is a politically exposed person (PEP). A PEP can present a higher risk of money laundering or terrorist financing. A PEP is an individual who has, or has had in the previous year, a high political profile, or holds, or has held in the previous year, public office overseas. Examples of PEPs include heads of state, heads of government, ministers, members of parliaments, members of supreme or constitutional courts or other high level judicial bodies, ambassadors and high ranking officers in the armed forces. The definition of PEPs extends to cover immediate family members and known close associates.

- whg will ensure that they have procedures in place to identify whether the customer is a PEP and take steps to establish the source of their funds which will be used during the business relationship or transaction. whg has in place procedures for senior managers to approve the establishment of a business relationship with a PEP. Where a business relationship is entered into, whg will undertake enhanced ongoing monitoring of the relationship. There is no all-encompassing list of PEPs but most electronic customer identification systems will check against their database to provide details of known PEPs.

Ongoing Monitoring

- Checks are carried out when a customer makes large or unusual cash payments to whg, for example to their rent account, or where they are purchasing a home or a share in a home. In the vast majority of cases there will be a reasonable explanation for the source of the funds, but unusual activity or transactions should be the catalyst for further enquiries to be made.

Persons that businesses must not accept as a customer

The Government may direct businesses not to enter into business relationships or transactions with certain individuals who are subject to financial sanctions. A list of all sanctions currently in force in the UK is maintained by The Treasury. This list can be found at: https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets

Situations where it is not possible to carry out due diligence

The Regulations are specific in relation to placing a requirement on businesses within the regulated sector to cease transactions where it has not been possible to carry out satisfactory checks in order to identify the customers. In those circumstances, whg:

- Must not carry out a transaction with or for the customer through a bank account
- Must not establish a business relationship or carry out an occasional transaction with the customer
- Must terminate any existing business relationship with the customer
- Must consider making a suspicious activity report to the National Crime Agency.

Record Keeping

whg's Data Retention Policy states that documents relating to a tenancy will be retained for six years after the end of the tenancy. This fulfils the legal requirement to keep evidence of a customer's identity for five years after the end of the relationship or the transaction.

In relation to customer identification, whg must keep:

- A copy of or details about the identification document presented and
- verification evidence obtained, or
- Information about where the evidence can be obtained.

If whg employs a third party to undertake its customer due diligence measures the business must ensure that the third party complies with the record-keeping obligations.

The purpose of keeping these records is to demonstrate whg's compliance with the Regulations and to aid any resulting investigations.

Records can be kept in a variety of methods such as original documents, photocopies of original documents, in computerised or electronic form. whg must also keep references as to where original documents can be found. How the records are retained will depend on how whg operates. whg must also keep records of internal and external reports and decisions as part of the Suspicious Activity Reporting (SAR).

In practice, it is recommended that the MLRO retains records in relation to colleague training and also records of any updates in respect of money laundering methods and legislation which have been disseminated to colleagues

Document author	Michael Cunneen, Policy and Compliance Officer
Document owner	Karen Marshall, Corporate Director of Governance and Compliance
Legal advice	Not required as no changes to legislation since the Policy was last reviewed
Consultation	N/A
Approved by	Audit and Assurance Committee April 2019
Review Date	October 2022
Corporate Plan aim	Deliver a strong business, fit for today and prepared for tomorrow
Equality analysis	N/A
Key changes made	• Legal and regulatory framework section updated including Governance and Financial Viability Standards and relevant legislation. • Ongoing monitoring added under Appendix 4.