Wheatley Group

Making homes and lives better
wheatley-group.com

Group Anti-Money Laundering and Counter-Terrorism Financing Policy

We will provide this policy on request at no cost, translated, in large print, in Braille, on tape or in another non-written format.

We can produce information on request at no cost in large print, in Braille, on tape or in another non-written format. We can also translate this into other languages. If you need information in any of these formats please call us on 0800 479 7979 or email info@wheatley-group.com

Możemy, na życzenie, bezpłatnie przygotować informacje dużą czcionką, w alfabecie Braille'a, na taśmie lub w innym niepisanym formacie. Możemy je również przetłumaczyć na inne języki. Jeśli potrzebujesz informacji w którymkolwiek z tych formatów, zadzwoń do nas pod numer 0800 479 7979 lub wyślij e-mail na adres info@wheatley-group.com

Podemos produzir informações mediante solicitação e sem custos, em impressão grande, Braille, cassete ou noutro formato não descrito. Também podemos traduzi-las em outros idiomas. Se precisar de informações em qualquer um destes formatos, contacte-nos através do número 0800 479 7979 ou envie um e-mail para: info@wheatley-group.com

يمكننا إنتاج معلومات عند الطلب مجانًا مطبوعة بأحرف كبيرة أو بطريقة برايل أو على شريط أو بتنسيق آخر غير مكتوب. يمكننا أيضًا ترجمة هذا إلى لغات أخرى. إذا كنت بحاجة إلى معلومات بأي من هذه التنسيقات، فيرجى الاتصال بنا على 0800 479 7979 أو إرسال بريد إلكتروني إلى info@wheatley-group.com

در صورت درخواست، می‌توانیم اطلاعات را در چاپ بزرگ، خط بریل، روی نوار یا در فرمت غیرنوشتاری دیگری ارائه دهیم. همچنین می‌توانیم اطلاعات را به سایر زبان‌ها ترجمه کنیم. در صورت نیاز به اطلاعات بیشتر در هریک از این فرمت‌ها، لطفاً از طریق شمارهٔ 0800 479 7979 با ما تماس بگیرید یا ایمیلی به info@wheatley-group.com ارسال کنید.

ہم درخواست پر معلومات کو بڑے حروف، بریل، ٹیپ پر یا کسی اور غیر تحریری صورت میں بغیر کسی لاگت کے مہیا کر سکتے ہیں۔ ہم اس کا دوسری زبانوں میں ترجمہ بھی کروا سکتے ہیں۔ اگر آپ کو ان میں سے کسی صورت میں یہ معلومات درکار ہوں تو برائے کرم ہمیں 0800 479 7979 پر کال کریں یا info@wheatley-group.com پر ای میل کریں۔

Approval body	*Group Audit Committee*
Date of approval	*14 August 2024*
Review Year	*2027*
Customer engagement required	*No*
Trade union engagement required	*Yes – For information*
Equality Impact Assessment	*No*

Contents

1. Introduction 3

2. Policy Aims 3

3. Policy Scope 5

4. Definitions: 6

5. Mitigating money laundering and terrorism financing risks 8

6. How to report suspicious activity 10

7. What happens to a raised concern 10

8. Equal Opportunities Statement 11

Appendix 1 – Suspiscious Activity Report 12

1. Introduction

Wheatley Housing Group and all of its Subsidiaries ('the Group') is committed to conducting its operations with honesty and integrity and will treat all reports of suspected money laundering or terrorist financing activities seriously. The Group has zero tolerance for such activities and all alleged instances will be investigated.

The Group Anti-Money Laundering and Counter-Terrorism Financing Policy (the Policy") is intended to provide staff and Board members with guidance about their responsibilities with regard to countering money laundering and terrorist financing activities, including how to report suspicious activities and how management will act on reported concerns.

2. Policy Aims

The Proceeds of Crime Act 2002 (POCA) applies to every individual within the United Kingdom and the commission of offences under POCA and the terrorism legislation carry severe penalties. For example, committing one of the principal money laundering offences carries up to 14 years' imprisonment and / or an unlimited fine. Any housing association will face money laundering risks associated with housing management and the everyday course of business. It is therefore important to have appropriate risk-based systems and controls to mitigate these money laundering and terrorist financing risks.

This Policy:

- Describes the responsibilities of all Board members and staff in relation to suspected money laundering and terrorism financing activities;
- Informs staff of the due diligence and record management controls used to mitigate the risk of money laundering and terrorism financing activities;
- Sets out the responsibilities of staff and managers in relation to anti-money laundering and counter-terrorism financing training, and the application of this policy;
- Informs Board members and staff about signs of money laundering and terrorism financing so that they can exercise vigilance;
- Describes the process for reporting of any suspicious activity; and
- Describes the process for investigation of reported suspicions.

Legal and Regulatory Framework:

This Policy takes account of relevant legal and regulatory requirements including:

- The Proceeds of Crime Act 2002;
- Economic Crime and Corporate Transparency Act 2023; and
- The Terrorism Act 2000.

Part 7 of the **Proceeds of Crime Act 2002** (POCA) provides for various money laundering offences. A person commits an offence if he or she:

- conceals, disguises, converts or transfers criminal property or removes it from England and Wales or Scotland or Northern Ireland;
- enters in to or becomes concerned in an arrangement which he or she knows or suspects facilitates the acquisition, retention, use or control of criminal property; or
- acquires, uses or has possession of criminal property.

Part 7 of POCA also requires financial institutions and businesses in the regulated sector to report to the UK Financial Intelligence Unit, which is part of the National Crime Agency (NCA), any suspicions about criminal property or money laundering. Even if a person is not in the regulated sector they must report any suspicions if they come across any suspicious activity through their trade, business or profession.

The **Terrorism Act 2000** (TA) criminalises both participation in terrorist activities and terrorist financing. In general terms, terrorist financing is:

- The provision or collection of funds;
- From legitimate or illegitimate sources;
- With the intention or in the knowledge;
- That they should be used in order to carry out any act of terrorism;
- Whether or not those funds are in fact used for that purpose.

The TA establishes a similar pattern of offences to those contained in POCA, i.e Principal terrorism offences of

- Fundraising,
- Use or possession,
- Arrangements,
- Money laundering,
- Failure to disclose offences, and
- Tipping-off offences.

All offences carry heavy criminal penalties. While the terrorist financing and money laundering regimes are different, they share similar aims and structures and run together in UK legislation. Many of the provisions of POCA and TA mirror one another and the definitions are deliberately matched.

The **Economic Crime and Corporate Transparency Act 2023** includes a new failure to prevent fraud offence to hold organisations to account if they profit from fraud committed by their employees. Under the new offence, an organisation will be liable where a specified fraud offence is committed by an employee or agent, for the organisation's benefit, and the organisation did not have reasonable fraud prevention procedures in place.

Policy Review

This Policy shall be reviewed at least every three years and more frequently where, for example, there is a need to respond to new legislation/policy guidance. Reviews will consider legislative, performance standard and good practice changes.

The Group will publish this policy on our staff intranet, WE Connect, and on our website. A hard copy is also available on request. Customers may also request a copy of the Policy in other formats and community languages.

3. Policy Scope

This Policy applies to all of the Group's activities. The responsibility to control the risk of money laundering or terrorism financing activities occurring resides at all levels of the Group and this policy covers all Board and Committee Members, employees, contractors and consultants.

Any Board member or employee suspected of being or found to be involved with money laundering or terrorism financing activities in the performance of their duties will be subjected to the Group's disciplinary procedures and may be reported to the Police or the National Crime Agency. The internal action in relation to both Board members and employees will be in addition to any prosecution proceedings that might occur.

Roles and responsibilities

The **Group Chief Executive** carries overall responsibility for the maintenance and operation of this Policy, including establishment of procedures for the detection and reporting of suspected money laundering and terrorism financing activities.

The **Director of Assurance** has delegated responsibility for management, review and improvement of the Policy and is the Group's ***Nominated Officer***, to whom all cases of suspected money must be reported at the earliest opportunity. As the Nominated Officer, the Director of Assurance will review the information received and decide if it needs to be reported to the NCA. Where the information received indicates there are reasonable grounds to suspect money laundering the Nominated Officer must inform the NCA at the earliest possible opportunity.

The **Director of Governance** is responsible for notifying appropriate Regulators of all reports of suspected money laundering or terrorism financing activities that result in a notifiable event, and how we are responding to them.

All **line managers** have day-to-day responsibility for the mitigation of money laundering and terrorism financing risks through:

- Identifying the money laundering and terrorism financing risks to which systems, operations and procedures are exposed;
- Designing and maintaining controls to mitigate those risks; and
- Notifying the Director of Assurance of any suspicious activity.

All **staff members**, including managers, are responsible for:

- Familiarising themselves with the contents of this Policy and completing the Group's mandatory Business Ethics e-learning module;

- Adhering to due diligence identification procedures for all Group customers on every occasion. This will mitigate the risks of the business being used to launder money or fund terrorism; and
- Reporting details immediately to the Director of Assurance if they suspect or believe that another person may be engaged in money laundering or terrorism financing activities.

4. Definitions:

Money laundering is the illegal process by which funds derived from criminal activity are given the appearance of being legitimate by being exchanged for clean money. That means that the proceeds of any acquisitive crime are 'cleaned up' by various means and then fed back into the financial system after a transaction or transactions designed to disguise the original source of the funds.

Terrorists need funds to plan and carry out attacks. ***Terrorist financing*** is providing or collecting funds, from legitimate or illegitimate sources, to be used to carry out an act of terrorism.

Typically, money laundering involves three stages:

Placement: The process of placing criminal property into the financial system. This might be done by breaking up large sums of cash into smaller amounts or by using a series of financial instruments (such as cheques or money orders) which are deposited at different locations (e.g. regular or large credit balances on tenants accounts).

Layering: The process of moving money that has been placed in the financial system in order to obscure its criminal origin. This is usually achieved through multiple complex transactions often involving complicated offshore company structures and trusts (e.g. transferring payments in and out of multiple rent accounts).

Integration: Once the origin of the money is disguised it ultimately must reappear in the financial system as legitimate funds. This process involves investing the money in legitimate businesses and other investments such as property purchases, share investments or setting up trusts (e.g. customers requesting refunds on credit balances > £100).

Money laundering activity includes:

- acquiring, using or possessing criminal property;
- handling the proceeds of crimes such as theft, fraud and tax evasion;
- being knowingly involved in any way with criminal or terrorist property;
- entering into arrangements to facilitate laundering criminal or terrorist property;
- investing the proceeds of crimes in other financial products;

- investing the proceeds of crimes through the acquisition of property/assets; and
- transferring criminal property.

Recognising suspicious activity

Typical signs of money laundering and terrorist financing are:

- Obstructive or secretive customers;
- Customers based a long way from the Group with no apparent reason for using the Group services;
- Complex or unusually large transactions. For example, a customer on housing benefit suddenly has the funds for a deposit to fund a house purchase;
- Money transfers where there is a variation between the account holder and signatory;
- Payments to or from third parties where there is no logical connection to the customer. 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 be the proceeds of crime; and
- Overpayment of money due and credit balances returned to customer.

Some other potential signs of money laundering include:

- ***The misuse of properties for criminal purposes***

All of the examples below could result in the proceeds of crime being used for rental payments.

  - Cannabis farms in properties can be a danger to other residents due to an increased fire risk.
  - 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 antisocial behaviour and danger to residents.

- ***Fraud (internal and external)***

Fraud, whether perpetrated by employees or from another source, also creates the proceeds of crime which are then laundered. Examples include:

  - Collusion fraud by contractors or suppliers to corrupt the tendering process or employees involved in such collusion.
  - Gratuities or incentives to employees as an incentive to award contracts.
  - Criminals setting up front companies or shell companies to defraud associations.

- Foreign lenders that are fronts for criminality posing as bona fide financial institutions to lend money to associations.

- ***Other forms of criminality***

There are a number of other criminal acts which have a direct impact on the sector and some examples are:

- vulnerable tenants being targeted by loan sharks (illegal lending);
- identity theft allowing criminals to perpetrate other crimes; and
- criminals exploiting the lack of adequate financial systems to obtain refunds after making overpayments in cash.

5. Mitigating money laundering and terrorism financing risks

In order to mitigate the risk that money laundering or terrorism funding activities as outlined in the previous section could occur within the business, the Group requires the following controls to be applied.

Customer Due Diligence checks

All staff should adhere to due diligence identification procedures on every occasion. All customers must be identified fully with two forms of valid identification. This must include photographic evidence of identity and evidence of their residence e.g. a council tax or utility bill dated in the last three months.

Should a face-to-face meeting not take place, nor electronic ID verification from independent and reliable sources be obtained, then enhanced due diligence procedures must be adopted. This includes asking for additional information or evidence to establish the customer's identity, and ensuring that the documents supplied are certified. It would also be prudent to ensure that the first payment is made to/from a bank account in the customer's name. Enhanced due diligence is also required when a client is established in a high-risk third country or a relevant transaction involved a client in a high risk third country.

If the verification of the customer's identity is via documents this should be based on:

- A Government issued document with the customer's full name and photograph with either the customer's date of birth or residential address such as:
  - Valid passport;
  - Valid photocard driving licence;
  - National identity card
  - Any other photographic ID, such as a bio-metric residence test.

- OR, a government issued document (without a photo) which includes the customer's full name and supported by secondary evidence:
  - Old style driving licence;

    - Recent evidence of entitlement to state or local authority-funded benefit such as housing benefit, council tax benefit, pension.
- Supported by secondary evidence such as
    - A utility bill;
    - Bank or building society statement;
    - Most recent mortgage statement from a recognised lender.

The secondary evidence should ideally be dated no more than three months prior to the date of the check.

Other Customers

For customers who are not private individuals, such as corporate customers and private companies, it is also necessary to establish the names of all directors (or equivalent) and the ultimate beneficial owners of such entities.

The Group must obtain information that is relevant e.g. company registration number, registered address and evidence that the individual(s) has the authority to act for the company – a search at Companies House will identify the directors and company secretary. If we become aware of any discrepancies between the information held by Companies House and our own records (based on the Companies House definition of a person of significant control), this must be reported to Companies House.

Where the Group has reason to believe or suspect, or has identified, that a customer is controlled or owned by a beneficial owner they should consider whether it is necessary to verify the beneficial owner's identity. In verifying the beneficial owner's identity, the Group should be satisfied that it knows who the beneficial owner is and understand how it operates. This may include finding out who has ownership or control over the funds, or who is the controlling mind by requiring the customer to provide information directly, making use of publicly available documents or verifying the identity of the beneficial owner by some other means. Advice on the steps required can be obtained from the Director of Assurance.

Record keeping

In order to demonstrate the Group's compliance with POCA and the TA, and to aid any resulting investigations, the following records must be kept for 5 years:

- Copies of, or references to, the evidence obtained of a customer's identity for five years after the end of the customer relationship, or five years from the date when the transaction was completed.
- Supporting records relating to a customer relationship or occasional transaction for five years from the date when the transaction was completed.

At the end of the five-year period you must delete any personal data in those records unless:

- you are required to retain records containing person data under an enactment or for the purposes of court proceedings or you have reasonable grounds for believing the records need to be retained for legal proceedings, or
- you have the consent of the person whose data it is.

Training

On joining the Group, staff will be required to read this Policy as part of their induction process. All staff will be required to read this Policy as part of the Group's Business Ethics e-learning module. Further training and support will be provided for staff raising concerns as required.

6. How to report suspicious activity

Understanding our customers is crucial. Unusual activity or transactions outside established norms should be considered as a potential indicator of suspicious activity. Examples of potentially suspicious activity are set out in section 4 of this Policy.

All staff members are obliged under the POCA to report any suspected money laundering and terrorist financing actvities. Failure to meet these obligations can lead to criminal penalties and substantial fines.

Staff must make a report to the Nominated Officer 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 activities. This report should be via an internal Suspicious Activity Report (SAR), as shown in Appendix 1.

Staff should guard against alerting a suspected launderer once they have made their report to the Nominated Officer. Where staff are unsure of how or whether to proceed with a transaction, advice should be sought from the Nominated Officer.

7. What happens to a raised concern

Upon receipt of a Suspicious Activity Report, the Nominated Officer will log and acknowledge receipt of the report within 3 working days.

The Nominated Officer will consider the report and any other available internal information they think relevant, including undertaking other reasonable inquiries, to ensure that all available information is taken into account in deciding whether a report to the National Crime Agency (NCA) is required.

The Nominated Officer will evaluate the disclosure report and any other relevant information, and decide whether:

- there is actual or suspected money laundering taking place; or
- there are reasonable grounds to know or suspect that is the case; and
- whether they need to seek consent from the NCA for a particular transaction to proceed.

If the Nominated Officer decides there are reasonable grounds to suspect money laundering, they will inform the NCA at the earliest possible opportunity. Where the Nominated Officer concludes that there are no reasonable grounds to suspect money laundering, the Nominated Officer will fully document the rationale behind any such decisions and retain those records.

All reports of suspicious activity will be treated as confidential and securely stored for a minimum of five years, regardless of whether they are reported onto the NCA or not.

8. Equal Opportunities Statement

This Policy complies fully with the Group's Equality and Diversity Policy. We recognise our pro-active role in valuing and promoting diversity, fairness, social justice and equality of opportunity by adopting and promoting fair policies and procedures.

We are committed to providing fair and equal treatment for all our stakeholders including tenants and will not discriminate against anyone on the grounds of race, colour, ethnic or national origin, language, religion, belief, age, sex, sexual orientation, gender re-alignment, disability, marital status, pregnancy or maternity.

We check policies and associated procedures regularly for their equal opportunity implications. We take appropriate action to address inequalities likely to result or resulting from the implementation of the policy and procedures.

Appendix 1 – Suspicious Activity Report

Required Information	Response
Date	
Name and designation of reporting individual	
Suspected persons	
Name	
Address / business address	
Telephone numbers	
Name of customer (if different)	
Details of relevant transaction	
Nature of suspicious activity Give full details of suspicion and date suspicion first aroused. Continue overleaf if necessary.	
Provide details of transactions and identify checks.	
Attach any relevant documents.	
Signature of reporting individual	
To be completed by Nominated Officer:	
Refer to NCA / Do Not Refer to NCA	
Date referred to NCA (if applicable)	
Reason for decision	
Signature	