Islington & Shoreditch Housing Association

ANTI-MONEY LAUNDERING (AML) POLICY

1. INTRODUCTION

1.1 Money laundering is a criminal process by which funds that have been derived from criminal activities are given the appearance of being legitimate by being exchanged for clean money or assets.

1.2 From 1 September 2022, the Money Laundering and Terrorist Financing (Amendment) (No. 2) Regulations 2022 created a new obligation for regulated entities to identify, assess and mitigate the risk of proliferation financing using a risk-based approach, similar to the treatment of other AML risks.

Proliferation financing is the act of providing funds or financial services for use, in whole or in part, in the manufacture, acquisition, development, export, trans-shipment, brokering, transport, transfer, stockpiling of, or otherwise in connection with the possession or use of, chemical, biological, radiological or nuclear weapons, including the provision of funds or financial services in connection with the means of delivery of such weapons and other Chemical, Biological, Radiological and Nuclear related goods and technology, in contravention of a relevant financial sanctions obligation.

1.3 This money may be the proceeds of any criminal activity including theft, fraud, drug dealing and trafficking, corruption, tax evasion, prostitution, terrorism, extortion or people trafficking.

1.4 In this way the proceeds of crime are “washed” and fed back into the financial and banking systems following a transaction, or series of linked transactions, that disguise the original source of funds and give the impression that the funds are legitimate.

1.5 Money laundering is illegal and those who participate in it with knowledge or withsuspicion commit criminal acts.Turning a blind eye to money laundering is not an option.

1.6 Money laundering is a crime to which all organisations are vulnerable. As a business operating in the real estate sector, ISHA may be particularly attractive to criminals.

1.7 ISHA is required to comply with anti-money laundering legislation in respect of certain of its activities. We are obliged to establish internal procedures to prevent the use of our services for money laundering purposes, put in place reporting mechanisms and provide training to staff.

1.8 This policy (the "AML policy") has been prepared in order to give guidance to staff on the obligations of ISHA and each individual staff member in respect of anti- money laundering. ISHA's anti-money laundering procedure (the "AML procedure") should be read in conjunction with this AML policy.

2. RELEVANT LEGISLATION

- Part 3 of the Terrorism Act 2000 (the "Terrorism Act")
- Part 7 of the Proceeds of Crime Act 2002 ("POCA")
- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the "MLR")
- The Criminal Finances Act 2017 ("CFA")
- The Economic Crime and Corporate Transparency Act 2023 ("ECCT Act")

3. WHO THIS POLICY APPLIES TO

3.1 This AML Policy applies across the organisation to all staff.

3.2 The requirements of the AML procedure only apply to those members of staff who are involved in relevant transactions ("Relevant Transactions"), albeit the AML Procedure also assists in the interpretation of this AML policy, and should therefore be read by all staff in conjunction with the AML policy. Relevant Transactions are transactions:

a) In the Regulated Sector. "Estate agency work" is within the Regulated Sector. This includes introducing / negotiating with people who want to buy or sell freehold or leasehold property that does not belong to the organisation that is buying or selling it. This will cover, by way of example, where ISHA introduces a purchaser to a vendor of a shared ownership property (i.e. resales) or where we are providing introduction services to other housing providers.
b) All property sales, which includes staircasing, Right to Acquire, Right to Buy and any other property sales which the Association will engage in.
c) Rent, service charges and all other letting related receipts.

which involves income for ISHA, where the source of funds is obviously not consistent with past behaviour.

3.3 Breaches of the AML Policy or the AML Procedure may amount to a criminal offence.

3.4 Failure by a member of staff to comply with this AML policy or the AML procedure may lead to disciplinary action being taken against them. Any disciplinary action will be dealt with in accordance with ISHA's disciplinary procedure.

3.5 Any member of staff who suspects that money laundering may be taking place involving any part of the organisation must report it immediately to the Money Laundering Reporting Officer (the "MLRO") or their deputy (the "Deputy MLRO") and otherwise must not discuss their suspicions with anyone else without the authority of the MLRO or the Deputy MLRO.

4. DEFINITION OF MONEY LAUNDERING

4.1 Money laundering offences under POCA involve knowing, or suspecting, that a specific item of property is a person's benefit from criminal conduct, when it is in fact that person's benefit from criminal conduct, and:

4.1.1 Concealing, disguising, converting, transferring or removing it from England & Wales, Scotland or Northern Ireland (section 327);
4.1.2 Entering into or being concerned in an arrangement which a person knows, or suspects, facilitates the acquisition, retention, use or control of it by or on behalf of another person (section 328); or
4.1.3 Acquiring, using or possessing it (section 329).

4.2 Additional money laundering offences under the Terrorism Act section 18 involve entering into or being concerned in an arrangement which facilitates the retention or control, by concealment, removal from England & Wales, Scotland or Northern Ireland or transfer to others, of property which is:

4.2.1 likely to be used for the purposes of terrorism;

4.2.2 proceeds of the commission of acts of terrorism; or

4.2.3 proceeds of acts carried out for the purposes of terrorism.

4.3 In addition, there are two other offences that might be committed:

4.3.1 Staff in the Regulated Sector failing to disclose knowledge or suspicion that a person is engaged in money laundering to the MLRO or the Deputy MLRO, failing to report a suspicion to the National Crime Agency ("NCA").

4.3.2 Any staff tipping off any person that such a disclosure has been made or tipping off a person who is suspected of being involved in money laundering either directly or indirectly in such a way that is likely to prejudice an investigation ("Tipping Off"). Discussing a matter with the MLRO or the Deputy MLRO is not likely to prejudice an investigation.

4.4 The penalties for these offences involve fines and significant custodial sentences, in some cases up to 14 years imprisonment.

4.5 These offences do not apply where the NCA has provided the appropriate money laundering defense. However, money laundering is not only a criminal matter.If money is laundered by ISHA, even with a money laundering defense, then ISHA exposes itself to a potential civil liability for the losses suffered by a victim of the underlying criminal offence.

5. MONEY LAUNDERING INDICATORS

5.1 It is impossible to be definitive on how to spot money laundering or on how to decide whether to make a report to the MLRO or the Deputy MLRO. Criminals are constantly developing new and more sophisticated ways to launder money.

5.2 Appendix 1 details examples of possible warning signs that may indicate that money laundering might be present. It is not a definitive list, and staff must use their own experience and judgment to consider individual cases.

5.3 ISHA does not receive cash payments for its services.

6. RESPONSIBILITIES

6.1 The MLR requires a risk-based approach and so ISHA is required to identify, assess and manage the risks that the business may be exposed to in respect of money laundering or terrorist financing in light of the type of regulated activities we are involved in, the size of the business and that we are operating in the social housing sector.

6.2 ISHA is obliged to do the following:

6.2.1 Register with HMRC.

6.2.2 Appoint an MLRO to receive disclosures from staff of money laundering activity (their own or anyone else's).

6.2.3 Appoint a member of the Leadership Team to be responsible for overall systems to ensure compliance with the MLR and supervise the MLRO (the "Officer for Compliance").

6.2.4 Implement a procedure to enable the reporting of suspicions of money laundering, including training of staff.

6.2.5 Undertake risk assessments both organisation wide and in respect of customers during each Relevant Transaction with such risk assessments to be kept under regular review.

6.2.6 Undertake screening of staff engaged to undertake Relevant Transactions to ensure they have relevant experience to identify the risks of money laundering, terrorist financing and proliferation financing. The association also undertake to provide regular training for this group.

6.2.7 Maintain client identification procedures/Customer Due Diligence in the business areas involving relevant transactions.

6.2.8 Maintain accurate record keeping procedures and retain records for six years from the end of a business relationship in respect of Relevant Transactions.

6.2.9 External independent internal audit to ensure compliance with the AML policy and AML procedure.

6.3 The end of a business relationship shall be:

a) Outright sale of the freehold of a property to an individual with no contractual obligations by ISHA or the individual.This will cover, by way of example, where ISHA introduces a purchaser to a vendor of a shared ownership property (i.e. resales) or where we are providing introduction services to other housing providers.
b) When the lease term expires and is not renewed.Rent, service charges and all other letting related receipts.
c) Termination of the lease before it expires either by mutual agreement or by giving the required notice or as may be determined by the court.

6.4 The implementation of procedures and processes to manage the obligations set out above can be found in the AML procedure.

6.5 ISHA have undertaken a risk assessment across the organisation, and the outcome of that risk assessment has fed into the AML policy and AML procedure.

6.6 The Board's role is to lead and embed a culture of zero tolerance of money laundering, approve the policy and monitor compliance and controls.

6.7 The Head of Finance has been appointed the MLRO and the Deputy MLRO is the Director of Housing and Neighbourhoods. The MLRO and the Deputy MLRO are accountable to the Officer of Compliance for day-to-day oversight and implementation of the AML Policy and the AML Procedure. The MLRO and the Deputy MLRO must provide guidance and assistance in order to ensure compliance and must deal with any suspicious activity reports to the NCA, as explained in the AML Procedure. They must also provide an annual report to the Board on the operation of the ISHA's money laundering systems, without giving detail of any specific cases, which must be kept confidential by the MLRO, Deputy MLRO and the Officer for Compliance.

6.8 The Finance Director is the Officer for Compliance. The Officer for Compliance will receive reports produced by the MLRO or the Deputy MLRO and will make recommendations for changes in the AML Policy and AML Procedure.

7. THIRD-PARTY RELIANCE AGREEMENT

7.1 As part of our customer due diligence (CDD) measures on the Shared Ownership 1st Tranche sales, we have established a third-party reliance agreement with independent financial advisers (IFAs) who are authorised and regulated by the Financial Conduct Authority (FCA). The list of the IFAs is maintained by the Sales & Marketing Team.

The IFAs are instructed to undertake fee-free CDD checks on our behalf in conjunction with the mandatory financial eligibility assessment that any prospective buyer must undergo. The CDD checks include verifying the identity, address, and source of funds of the buyers, as well as screening them against any foreign politically exposed persons (PEPs) or sanctions lists. The results of the CDD checks are then sent to ISHA by the IFAs for review and approval. We retain copies of all CDD records provided by the IFAs on our own files for at least six years after the end of the business relationship.

For the Leasehold sellers of relevant properties, prior to marketing of a resale ISHA requires provision of current photo ID (Passport or Driver's License) and a recent utility bill with the appropriate name and address. These requirements are detailed in the guidance document provided to leaseholders upon initial enquiry.

We have obtained written confirmation from each IFA that they apply CDD measures that are consistent with the requirements of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017).

We are aware of our responsibility to consider the risks of proliferation financing and to apply enhanced due diligence measures where appropriate. We rely on the IFAs to inform us of any potential proliferation financing risks that they may identify during the CDD process. We also monitor the guidance and updates from the gov.uk website and the Financial Action Task Force (FATF) website on this matter.

It should be noted that where ISHA relies upon a third party to carry out customer due diligence, ISHA will remain primarily liable under the Regulations for any failure by that third party to complete the due diligence adequately. Managers should therefore ensure they also review the documents and satisfy themselves of the adequacy.

PEP risk differentiation

In line with the 2024 MLR amendments, ISHA will:

- Apply enhanced due diligence (EDD) only to high-risk domestic PEPs.
- Continue strict monitoring of foreign PEPs.
- Conduct ongoing risk assessments to determine when EDD is necessary.

8. TRAINING

8.1 ISHA is committed to zero tolerance of money laundering and in accordance with our obligations, we will ensure that:

8.1.1 All staff are aware of the AML policy and AML procedure and of the obligation to implement it.
8.1.2 All staff involved in Relevant Transactions are trained in the AML procedure.

8.2 It is the responsibility of the MLRO to ensure that all staff are appropriately trained and are aware of this AML policy and the AML procedure.

9. REVIEW

4.1 This policy will be reviewed every year or following changes to legal requirement.

ANTI-MONEY LAUNDERING (AML) PROCEDURE

10. INTRODUCTION

10.1 ISHA has a zero-tolerance attitude to money laundering. This AML procedure sets out ISHA's expectations of its staff involved in Relevant Transactions and their duties in relation to the prevention of money laundering.

10.2 This procedure supplements the AML policy, which should be read together with this document. The definitions in the AML policy have been adopted in this document.

10.3 The checks set out in this AML procedure should be carried out by a member of staff involved in a Relevant Transaction before they enter into a contract with ISHA.

10.4 All staff have a duty to report any suspicious activity related to money laundering to the MLRO or the Deputy MLRO who will then decide whether or not to make a report to the NCA.

10.5 The purpose of the AML procedure is to put in place systems and checks that significantly increase the likelihood that money laundering is detected, in order to allow suspicions then to be reported as appropriate. However, it is up to each person to use their own knowledge and experience to determine if money laundering is suspected or taking place. If in doubt, a report should be made, so that the MLRO or the Deputy MLRO can then decide what further action is required.

10.6 It is important that staff involved in Relevant Transactions fully understand their responsibilities under the legislation. They are required to follow this AML procedure and to make a report to the MLRO or the Deputy MLRO if they have a suspicion that money laundering is, or has been, taking place. Once they have reported their suspicions to the MLRO or the Deputy MLRO, staff must not make any further enquiry into the matter or discuss the matter further with anyone save under the express direction of the MLRO or the Deputy MLRO. On no account must they make reference to their suspicions on a personnel, tenant, or other file or electronic document management system. The only permitted file to hold this information is the permanent file securely maintained by the MLRO or the Deputy MLRO.

11. KEY REQUIREMENTS

10.1 There are four key requirements to meeting our obligations:

10.1.1 Customer due diligence checks.

10.1.2 Reporting knowledge or suspicions:

10.1.2.1 to the MLRO or the Deputy MLRO
10.1.2.2 if appropriate, from the MLRO or the Deputy MLRO or to the NCA.

10.1.3 Maintaining records; and

10.1.4 Training staff involved in Relevant Transactions in the procedures for recognising and reporting knowledge or suspicions of money laundering.

Customer due diligence checks

10.2 Exercising customer due diligence (Knowing Your Customer) is an essential element in protecting against money laundering activities.The purpose of this exercise is to put the member of staff in the best possible position to detect possible money laundering.The focus should not be the obtaining of this material, which should be automatic, but what the material reveals once it has been obtained.

10.3 ISHA will seek to ensure that it only deals with bona fide individuals and organisations.

10.4 Before commencing any Relevant Transaction.

10.4.1 with any new customer or business partner,

10.4.2 with an existing customer or business partner, if only occasional Relevant Transactions are undertaken with them,

10.4.3 if there is a suspicion of money laundering; or

10.4.4 If there are doubts about the validity or adequacy of documents already held.

ISHA must:

10.4.5 Verify the identity of all persons and businesses involved in the transaction, including the ultimate beneficial owner of those businesses, undertaking enhanced checks where appropriate; and

10.4.6 Establish the source of their money.

10.5 Satisfactory evidence is evidence that is capable of establishing, to the satisfaction of the person receiving it, that those involved in the Relevant Transaction, including eventual beneficial owners, are who they claim to be, and that the source of their money is legitimate. If such satisfactory evidence cannot be obtained, then ISHA must not enter into the Relevant Transaction. It may also lead to a suspicion of money laundering, depending on why the evidence cannot be obtained.

10.6 Appendix 2 contains guidance as to the list of documents for use in establishing identification. This also sets out the circumstances in which enhanced checks are appropriate, and where ISHA cannot transact at all.

Understanding source of monies involves common sense. It requires asking where the money comes from and keeping copies of the evidence. For example, for property transactions, we could ask the question and be told there will be a mortgage and the deposit will be a parental gift. For this we would need to keep copies of paperwork from the mortgage company as well as a letter from the parent, accompanied by their bank statement or similar showing that they had the money to give, and evidence from them to demonstrate the money's legitimacy.

10.7 Occasional transactions with an existing individual or organisation are just as important as new individuals / organisations. Just because there were legitimate funds for a transaction 5 years ago does not mean that new funds are legitimate today.

Reporting knowledge or suspicions – To the MLRO or Deputy MLRO

10.8 Any staff member who is involved with any proposed Relevant Transaction needs to consider whether they ought to have a suspicion of money laundering.

10.9 Where the staff member has a suspicion that money laundering may be intended or has been committed, then they must report the suspicion to the MLRO Team immediately.Failure to do so is likely to be a criminal offence.

10.10 Any suspicions must be reported to the MLRO or the Deputy MLRO on the internal Suspicious Activity Report (SAR) form at Appendix 3. Ideally this document should be delivered to the MLRO or the Deputy MLRO personally. Anonymous reports may be submitted but where the identity of the reporter is not given, it will not provide the employee with the necessary evidence of compliance with their obligations as they will require under the MLR. No copy or note of the report should be held in any personnel, tenant, or other file or electronic document management system. The only permitted file is the permanent file securely maintained by the MLRO or the Deputy MLRO.

10.11 It is a criminal offence to advise a person that the authorities have been advised of suspicions of the transaction, or to give information directly or indirectly to a suspect which may prejudice an investigation, so called Tipping Off. Criminal penalties are severe and where a suspicion has been raised, this fact must not under any circumstance be communicated to the suspected person nor to anyone other than the MLRO or the Deputy MLRO, unless the MLRO or the Deputy MLRO then provides express direction as to any further action to be taken.

Reporting knowledge or suspicions – By the MLRO or Deputy MLRO

10.12 The MLRO or the Deputy MLRO will, as soon as practically possible, review the information on the report and make their own enquiries if necessary. Amongst other things, in making a decision as to whether they have a suspicion of money laundering, the MLRO or the Deputy MLRO will consider:

10.12.1 Whether the conduct under scrutiny falls within that which is potentially criminal.

10.12.2 If so, whether the money intended to be used for the Relevant Transaction is suspected of being the proceeds of that conduct; and

10.12.3 The disclosure report and any other internal information available to him/her and undertake such other reasonable enquiries he/she thinks appropriate in order to ensure that all available information is taken into account before deciding if a report to the NCA is required. This may include the MLRO undertaking enhanced checks as set out in Appendix 2 by seeking alternative verification and other evidence better to understand the position. It may also include discussing the matter with the member of staff that has made the report and directing further investigations to be made by them.

10.13 The MLRO or the Deputy MLRO must reach a conclusion as to whether they do, or do not have reasonable grounds to suspect money laundering.

10.14 If the MLRO or the Deputy MLRO concludes that actual or suspected money laundering is taking place then, unless there are lawful grounds for non-disclosure, the matter must be disclosed to the NCA via the confidential reporting website http://www.ukciu.gov.uk. If the MLRO believe that there are lawful grounds for non-disclosure, they must be very certain about this, if necessary obtaining legal advice, as such grounds are limited and rare.

10.15 If the MLRO or the Deputy MLRO suspects money laundering but has lawful grounds for non-disclosure to the NCA or concludes there are no reasonable grounds to suspect or confirm money laundering, the internal disclosure report must be annotated accordingly with the reasons for the decision. Consent can then be given by the MLRO or the Deputy MLRO for any on-going or imminent transactions to proceed, if appropriate, taking into account potential civil liability and other risks faced by ISHA.

10.16 The MLRO or the Deputy MLRO may consider it necessary to seek a money laundering defence from the NCA to any money laundering offence, potentially allowing a transaction to

proceed, taking into account potential civil liability and other risks faced by ISHA.In such a case the transaction may not be undertaken until the NCA has specifically given the defense or there is a deemed defense through the expiration of the relevant time limits laid down for the notice or moratorium periods (see below) without NCA objection.For the avoidance of doubt, a money laundering defense does not give any immunity to civil liability – indeed, in many circumstances it may make that liability more certain, because obtaining such a defense necessitates the MLRO or the Deputy MLRO identifying and refining all their suspicions of money laundering in circumstances where those suspicions themselves may lead to civil liability if the transaction proceeds.

The NCA has seven working days starting the first working day after the defense is requested to refuse. If the defense is refused, a further 31 days (the “Moratorium Period') starting with the day of refusal must elapse before activity may continue with a deemed defense. This Moratorium Period can be extended and re-extended by Court order for up to 31-day intervals, up to a maximum of a further 186 days. The NCA will ordinarily contact the MLRO Team direct by telephone with the decision and post an appropriate letter as confirmation. The reality is that, if the NCA intend to refuse, they will extend the Moratorium Period for as long as possible and, in the meantime, seek a “restraint order” which is then served on ISHA, thereby freezing the criminal’s assets and stopping any transaction from proceeding.

Maintaining records

10.17 To demonstrate compliance with the MLR, ISHA will keep records as below:

10.17.1 Copies of the evidence obtained of a customer's identity and source of funds will be kept for six years after the end of the relationship and, for occasional transactions, for six years after the transaction was completed. Thereafter it must be destroyed in accordance with ISHA’s data obligations, unless there is lawful reason to the contrary.

10.17.2 Details of our residents will continually be updated using the following methods.

10.17.2.1 Confirmation of the correctness of the contact details held on our system by the Customer Service Team when dealing with our residents.

10.17.2.2 Income Team and Finance Team keeping an eye on residents financial transactions and flagging unusual or significant changes in transaction patterns which might indicate suspicious activity and reviewing the highlighted resident's information and documentation to ensure it's up to date. This includes verifying their source of income, employment status, and any changes in their financial situation.

10.17.2.3 Behavioral analysis: Neighbourhoods Team to highlight any behavioral changes and other red flags that might indicate potential involvement in illegal activities during their visits to our estates. This could include sudden changes in lifestyle, unexplained wealth, or evasive behavior during interactions.

10.17.3 Only the register and file maintained by the MLRO, or the Deputy MLRO is permitted to keep material relating to money laundering reports, both internal and to the NCA. No copy of any such report or note of its existence shall appear in any personnel, tenant, or other file, electronic or otherwise.

10.18 The MLRO or the Deputy MLRO will maintain a register recording all details of suspicious activity reported to them, all investigations and the action taken as a result, whether reported to the NCA or otherwise. This will be kept by the MLRO or the Deputy MLRO in a confidential file for that purpose and kept in compliance with the requirements of the Data Protection Act for at least six years from the conclusion of the investigation. There is no prescribed format for such records, but they must be capable of providing an audit trail during a subsequent investigation.

APPENDIX 1

MONEY LAUNDERING RISK INDICATORS

The following are types of risk indicators that may, either alone or together with other indicators, suggest the possibility of money laundering activity. The list is not exhaustive and the presence of a risk in the list below does not in itself mean that any illegal activity is being undertaken:

1 Checking a new customer's identity is difficult.

2 The size of the transaction is not consistent with previous activity. For example, a customer on housing benefit suddenly has the funds for a deposit to fund a house purchase.

3 The financial circumstances of an existing customer have changed dramatically.

4 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.

5 The customer wants to pay a large sum in cash.

6 A customer who puts pressure on you to accept his or her business before you can carry out the necessary checks.

7 A customer makes an approach to purchase a property then backs off on realising his or her identity will be checked for anti-money laundering purposes.

8 Large online payment or significant unexplained overpayments by a customer/client and subsequent requests for refunds, especially if this is a recurring event or the refunds are to be paid to another bank account.

9 Absence of a legitimate explanation of source of the funds.

10 A transaction or series of transactions, without obvious legitimate purpose or which appears uneconomic, inefficient, illogical or irrational.

11 Requests for release of bank account details other than in the normal course of business.

12 Poor business records or internal accounting controls.

13 Offers of goods or services or loans at below market prices.

14 Concerns about the honesty, integrity, identity or location of a client.

15 Previous transaction for the same client that has been, or should have been, reported to the MLRO.

16 In respect of property transactions, funds received for deposits or receipts prior to completion from an unexpected source or where instructions are given for settlement funds to be paid to an unexpected destination.

17 In shared ownership sales, the subsequent rapid staircasing and re-sale of the property.

APPENDIX 2

IDENTIFICATION CHECKS

All private individuals

1 For customers that are private individuals, the business should obtain full names, residential addresses and their date of birth.

2 Verification of this information must be based on reliable independent sources. This may be by documents provided by the customer or information obtained electronically by the business or both. All verification must either be in date (e.g. an in date passport) or dated within the last 3 months (e.g. a bank statement).

3 If the verification of the customer's identity is done by documents:

3.1 this should be based on a government-issued document with the customer's full name and photo, with either the customer's date of birth or residential address, such as valid passport, valid photocard driving license, national identity card, firearms certificate, identity card issued by the Electoral Office for Northern Ireland, or

3.2 where the customer does not have the above documentation, you can accept:

3.2.1 a government issued document (without a photo) which includes the customer's full name, such as:

3.2.1.1 old style driving license;

3.2.1.2 evidence of entitlement to state or local authority- funded benefit such as housing benefit, council tax benefit, pension, tax credit, pension, educational or other grant;

3.2.1.3 instrument of a court appointment (such as liquidator, or grant of probate);

3.2.1.4 current council tax demand letter, or statement; and

3.2.2 evidence of the customer's address, such as a utility bill, bank, building society or credit union statement or most recent mortgage statement from a recognised lender.

4 Sufficient checks should be made of the documentary evidence to satisfy the business of the customer's identity. This may include checking spelling of names, validity, photo likeness, whether addresses match etc.

5 Where a member of staff has visited the customer at his or her home address a record of this visit may constitute evidence of corroborating the individual's residential address (for the purposes of the evidence of the customer's address).

6 If the verification of the customer's identity is done by electronic means the business should undertake these checks from two separate sources. A copy of the electronic check should be retained, or information recorded as to where a copy of the evidence can be found.

7 When a member of ISHA's staff has not been able to meet the customer in person, ISHA can choose to accept certified copies of identification documents. A certified copy must be no more than three months old, certified by a UK solicitor, who appears on the roll of The Law Society of England & Wales or of Scotland, a chartered accountant on the roll of the Institute of Chartered Accountants of England and Wales (ICAEW), an accountant or a lawyer of another jurisdiction whose credentials you have verified through their relevant professional directory, or certification by a British Embassy or consular official. You must ensure that you receive a hard copy ('wet-ink') of the certified copy, which is signed and dated by the individual certifying it. A scan of the certified copy is not sufficient.

8 To accept a certified copy certified by any other third party, you must first obtain approval of the MLRO Team. A request for approval must state the reason for using the third party and who it is you are proposing to obtain the certified copy from, and that request, together with the annotated decision should be kept in the records held by the MLRO Team.

The above is applicable to all private individuals including current residents.

Customers other than private individuals

9 The definition of **Politically Exposed Persons (PEP)** is wide, but can be summarised as follows:

9.1 Individuals entrusted in the preceding year with prominent public functions including government ministers, their assistants, judges, boards of central banks or prominent state-owned enterprises, senior politicians or state officials.

9.2 Those individual's immediate family members and persons known to be their close associates. A "known close associate" extends to someone who has close business relations with a PEP or jointly owns a business with them; and

9.3 Assets held jointly with those individuals or by those individuals on behalf of the PEP.

9.4 **Domestic PEPs** are individuals who hold prominent public functions within the United Kingdom. Domestic PEPs are now classified as lower risk, requiring simplified due diligence, unless risk factors indicate otherwise.

9.5 **Foreign PEPs** are individuals who hold prominent public functions in foreign countries.

9.6 Initial Assessment: Domestic PEPs will be classified as lower risk by default. Foreign PEPs are considered high risk. Factors such as involvement in high-risk sectors, previous allegations of corruption, or significant control over public funds will elevate a domestic PEP's risk level.

10 For customers that are not private individuals, such as corporate customers, partnerships, and private companies, the business must obtain information that is relevant to that entity which includes:

10.1 the full name of the company;

10.2 company or other registration number, and

10.3 registered address and principal place of business.

11 This should be verified from reliable independent sources (relevant to that entity type) such as a search of a relevant company registry, confirmation of the company's listing on a regulated market, or a copy of the company's certificate of incorporation.

12 It is also necessary to establish the names of all directors (or equivalent) and the ultimate beneficial owners of such entities. Where we have reason to believe or suspect, or has identified, that a customer is controlled or owned by a beneficial owner we should identify that beneficial owner.

13 All ultimate beneficial owners holding more than 25% should then be verified in the same way as private individuals, unless documentary evidence is obtained to demonstrate that the entity is one of the following:

13.1 Listed on the London Stock Exchange, an EEA Stock Exchange, a USA Stock Exchange or AIM;

13.2 A wholly owned and consolidated subsidiary of such a listed company

13.3 An FCA regulated credit or financial institution

13.4 A professional regulated partnership; or

13.5 A public Authority, Institution or other public body.

14 In addition, you must verify the identity of the individual who is representing the entity in the same way as private individuals, and obtain satisfactory evidence that they are authorised by that entity to represent them.

Enhanced checks

15 In circumstances where you have assessed a party to be higher risk, enhanced evidence of identity and additional details should be sought. The situations which trigger a requirement for enhanced checks are:

15.1 You doubt the documentary evidence supplied, for example if an address on a driving licence and an address on a utility bill do not match and the party cannot explain this discrepancy

15.2 There is no face-to-face contact with the party.

15.3 Any aspect of the proposed transaction is suspicious, for example the source of funds for a transaction.

15.4 The transaction includes any domestic PEP who is involved in high-risk sectors, previous allegations of corruption, or significant control over public funds will elevate the risk level. This also includes the member of their family or a known associate; and/or

15.5 The transaction includes any foreign Politically Exposed Person (PEP) (see below), a member of their family or a known associate; and/or

15.6 The transaction involves any offshore company, or the structure is complex.

15.7 An individual is not a British Citizen and is from a high-risk country, such as a known tax haven or a country subject to international sanctions (Her Majesty's Treasury (HMT) publishes a list of high-risk countries from a money laundering perspective. The current list of high-risk countries 2023.

15.8 A customer has not been honest with you about the transaction or has provided false or stolen identification documentation.

15.9 The transaction is unusually large or complex or is part of an unusual pattern of transactions.

If the checks are not satisfactory in any of the above situations, the transaction should not continue. The case should be escalated to the appropriate manager. The manager should also consider reporting this to the MLRO in accordance with the anti-money laundering policy.

16 In order to undertake enhanced checks, you will need to consider the types of further documentation which should be required on the basis of the profile of the party. Additional documentation could include further background information, further information about the source of funds, details of an individual's source of wealth or a request for further documentation linked or referred to in the initial set of documentation. The nature of the enhanced checks will depend on the specific individual and their set of circumstances.

17 In the first instance staff must make enquires of the customer as to whether they, a close family member or a business associate is a high-ranking public official who could fall within the definition of a foreign PEP.

18 If a foreign PEP is involved, you are obliged to do the following:

18.1 To obtain approval from the Leadership Team to establish a relationship with the individual.

18.2 Take adequate measures to establish the source of wealth and source of funds involved in the transaction; and

18.3 Ensure that the individual is subject to ongoing monitoring until the end of the business relationship.

19 Once the identity has been verified, it should be checked against the HM Treasury sanctions list. The current consolidated list.

20 ISHA cannot transact with any individual or entity that is found on this list.

APPENDIX 3

INTERNAL SUSPICIOUS ACTIVITY REPORT (SAR) FORM

This report needs to be made as soon possible after becoming aware of the suspicious activity (within hours, rather than days or weeks later).

You must not make any further enquires or progress the transaction further without approval from the MLRO Team.**DO NOT** voice your suspicions to the suspect or anyone else or let them know an activity has been reported. Only discuss this matter with the MLRO or the Deputy MLRO.

Please attach all relevant documents.

When completed, **DO NOT** keep a copy of this form on any personnel, tenant, or other file, electronic or otherwise.

Your details	
Name	
Department	
Date of report	
Contact details	

Suspected person/company	
Identity of person	
Address of person	
Contact details of person	
Identity of company (if any)	
Address of company (if any)	
Contact details of company (if any)	

Nature and details of suspected offence

Include whether this has already occurred or is likely to occur, where / when this occurred and how it arose. Include details of all proposed or actual transactions.

Investigations

Have any investigations already occurred e.g. which have led to your having a reasonable suspicion? If so, please detail below.

Discussions

Have you discussed your suspicions with anyone, including any advisory bodies? If so, please give details. This should not be interpreted as a consent to discuss your suspicion with anyone else.However, if you have so discussed it, the MLRO or the Deputy MLRO need to know.

Further information
If there is any further information you believe to be relevant, please include here.
Please deliver this report to the MLRO or the Deputy MLRO immediately.

Reference	Version	Created	Author	Review	A&R approved
Anti-money laundering policy and procedure	2	January 2025	Head of Finance	January 2026	February 2025