LONDON BOROUGH OF TOWER HAMLETS

ANTI-MONEY LAUNDERING POLICY AND GUIDANCE

LONDON BOROUGH OF TOWER HAMLETS

ANTI-MONEY LAUNDERING POLICY AND GUIDANCE

APPENDIX B - Identity Verification Forms

APPENDIX C - Disclosure forms

IT IS OUR POLICY TO ENSURE THAT THE COUNCIL AND ITS OFFICERS AND EMPLOYEES ARE COMMITTED TO COMPLYING WITH ALL LEGISLATION AND APPROPRIATE GUIDANCE DESIGNED TO COMBAT MONEY LAUNDERING AND TERRORISM ACTIVITIES.

1 THE SCOPE OF THIS POLICY

1.1 This Policy applies to all officers and employees of London Borough of Tower Hamlets (**the Council)** and the Council's Arms Length Management Organisation ('ALMO'), Tower Hamlets Homes. The Policy sets out the procedures that must be followed to enable the Council to comply with its legal obligations and the consequences of not doing so. Within this policy the term 'persons' shall be used to refer to all officers and employees, both permanent and temporary, of the Council.

1.2 All persons must be familiar with their legal responsibilities. **Failure to comply is a criminal offence.**

1.3 The Council views compliance with the money laundering legislation as a high priority and aims to develop a robust and vigilant anti-money laundering culture. Money launderers are seeking to infiltrate reputable organisations including local authorities. Organisations perceived as having weak controls will be targeted first. Significant damage will be caused to the Council's reputation if it were to be associated, however innocently, with laundering the proceeds of crime, particularly if a person working within the Council was subsequently prosecuted.

1.4 Even if the Council is used as an innocent vehicle for money laundering, the cost of being involved in an investigation, both in terms of legal monetary fees, business disruption and overall reputational damage would be considerable.

1.5 It is therefore essential that all persons follow the Council's money laundering procedures in this Manual to ensure compliance with the relevant statutory regulations.

1.6 Failure by any person to comply with the procedures set out in this Policy may also lead to disciplinary action being taken against them. Any disciplinary action will be dealt with in accordance with the Council's Disciplinary Policy and Procedure.

1.7 All persons will be provided with a copy of this policy and are required to sign to confirm that they have received, read and understand the policy.

1.8 The Money Laundering Reporting Officer (**MLRO**) is Kevin Bartel, Interim Corporate Director of Resources (s151 officer) **, Corporate Anti-Fraud Manager** who is responsible for the day to day implementation and monitoring of this policy. However, all key senior officers recognise that they are ultimately responsible for ensuring that the Council's control processes and procedures are appropriately designed and implemented and effectively operated to reduce the risk of the Council being used in connection with money laundering or terrorist financing.

1.9 This Policy should be read in conjunction with the Council's Anti-fraud and Corruption strategy.

1.10 This Policy Guidance is updated incorporating amendments made to the Terrorism Act 2000, the Proceeds of Crime Act 2002 and the Money Laundering Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 as a result of the European Union's (EU) 5th Money Laundering Directive (Directive (EU) 2018/843) which came into force on 30 May 2018 and the exit of the United Kingdom from the European Union on 31 December 2020. These amendments were made by the Money Laundering and Terrorist Financing (Amendment) Regulations 2019 SI 2019 No 1511 and the Money Laundering and Terrorist Financing (Amendment) (EU Exit) Regulations 2020 SI 2020 No 991 respectively.

2 INTRODUCTION - WHAT IS MONEY LAUNDERING?

2.1 The phrase 'money laundering' means the process by which the identity and true ownership of 'dirty money', i.e. the proceeds of any crime, is changed so that these proceeds appear to originate from a legitimate source.

2.2 Most crime, for example the drugs trade, is almost wholly cash driven. For many years, the most common means of laundering money was to deposit large sums of cash at banks. However, as the high street banks have tightened their controls in this area, the launderers have turned to more obscure methods, frequently involving buying and selling assets, property and businesses, often via complex transactions, sometimes across geographical boundaries, to achieve their aims. This has made it much more difficult for the enforcement authorities to detect and prevent money laundering.

2.3 If you are involved, in any way, in dealing with or facilitating an arrangement with regard to 'criminal property', you are engaged in the offence of money laundering. 'Criminal property' is the proceeds of *any* crime under UK law. It is not limited to dealing in cash. If you handle the benefit of acquisitive crimes such as theft, fraud and tax evasion, or are involved in handling or processing stolen goods or assets purchased with the proceeds of crime, from cars to paintings and antiques, you are money laundering.

2.4 Terrorists also need to launder money to fund their criminal enterprises. The atrocities of 9/11 and terrorist bombings in London in July 2005 have focused attention on the need to enforce anti-money laundering rules to combat terrorists, as well as drug dealers and organised crime.

2.5 All regulated businesses must to adopt a risk-based approach, taking into account the contents of their practice-wide risk assessment, policies and procedures (and where necessary updating them) and the circumstances of business transactions. This will be implemented and overseen by the MLRO.

2.6 As well as changes to how we live our lives, COVID-19 is also changing the economy. An economic downturn may make individuals and businesses more susceptible to financial difficulties or other pressures, which creates risk and potential weaknesses for criminals to exploit. As the UK economy enters a period of uncertainty, employees must be particularly alert to the dangers of money laundering.

3 THE LAUNDERING PROCESS

3.1 The money launderer will seek to launder 'dirty money' via a series of transactions to separate the direct (usually cash) proceeds of an offence from the final bank account. Passing the funds through different accounts/investments and transferring it into different guises helps to muddy the audit trail.

3.2 There are three distinct, recognised phases to the laundering process:-

3.2.1 **Placement** - the initial disposal of cash representing the proceeds of crime into the system by deposit at a bank or similar but increasingly likely to involve the purchase of property, or other assets such as a business.

3.2.2 **Layering** - to break any link back to the direct proceeds of the crime. This is done by a variety of routes, including buying and selling properties, companies or assets (such as shares, antiques and art) back to back and transferring funds around the world via various accounts in many institutions. Often launderers will use a front company, carrying on legitimate business, to hide their illegal activities.

3.2.3 **Integration –** having gone through the transaction merry-go-round, the funds can come back to the individual criminal or their organisation, to finance a luxurious lifestyle, purchasing property, expensive cars, income-generating securities etc. and perhaps to fund further criminal activity.

4 HOW THE COUNCIL COULD BECOME INVOLVED IN MONEY LAUNDERING

4.1 The Council carries out transactions for a variety of purposes during which it handles money from customers. These transactions include (but are not limited to), dealings with leaseholders, payments for Council Tax and Business Rates, income from disposal of Council assets, right to buy deposits and financial contributions from planning legal agreements.

4.2 It is feasible for the Council to become unwittingly involved in the money laundering process via contacts who are carrying out apparently normal transactions, if the money, property or other assets they bring to the transactions are the proceeds of crime.

4.3 Examples;

4.3.1 Acquiring property which represents or has been purchased using the proceeds of a fraud, including false accounting. This could arise, for example, in the context of a procurement contract.

4.3.2 Handling (even if only as intermediary) funds which were not declared as required by law under an insolvency arrangement or were acquired by tax or benefit fraud.

4.3.3 Any similar dealing with funds obtained as a pay-off following threats to expose illegal or immoral behaviour.

4.3.4 Acquiring funds from a customer for buy to let properties which represent the proceeds of drug dealing

4.4 This is not an exhaustive list. As set out above, because the definition of money laundering is very wide, any contact with the proceeds of any offence, from petty theft to tax evasion, extortion and murder, is likely to constitute money laundering.

4.5 Where fraud or corruption is suspected, staff members will also need to follow the guidance set out in the Councils Anti-fraud and Corruption Strategy.

4.6 Any member of staff who deals with cash paid in by external parties must be alert to the possibility of council financial systems being used to launder "cash" (which is defined as "notes, coins or travellers' cheques in any currency").

4.7 Risk assessments should also be reviewed to money laundering, terrorist financing, bribery and corruption in the respect of Covid-19 and the consequent changes to the business environment and the economy. The Local Authority should be alert to financial scams and business relationships with those susceptible to monetary difficulties or other pressures, which could create risk and potential weaknesses for criminals to exploit.

4.8 Accountants, auditors and legal officers must be especially alert to the possibility of council financial systems being used to launder cash, particularly if significant sums are involved, such as the purchase price for council property**.**

4.9 Legal practices and regulated businesses should be aware that criminals will continue to operate throughout, and look to take advantage of, the Covid-19 outbreak. This includes laundering the proceeds of crime and terrorist financing, so it is important that everyone is aware of the changing risks

4.10 As the UK economy enters a period of uncertainty, employees should be particularly alert to the following risks in new or prospective customers. For example,

(a) being asked to work with unusual types of client or on unusual types of matter,

(b) resistance from a client regarding compliance with due diligence checks,

(c) being pressured to forego necessary due diligence checks or to "speed up" the process,

(d) becoming involved in work that is outside of their normal area of experience/expertise (without full understanding of the money laundering and counter terrorism risks associated with the new area of work)

(e) transactions where the business rationale for the transaction is not clear

RIGHT TO BUY TRANSACTIONS, PROCUREMENT AND COMMERCIAL AGREEMENTS ARE ALSO SUSCEPTIBLE TO MONEY LAUNDERING. THEREFORE, STRINGENT CHECKS ARE REQUIRED TO ASCERTAIN IDENTITY, THE SOURCE OF FUNDS, THE LEGITIMACY OF TRANSACTIONS (AS A MINIMUM), TOGETHER WITH OBTAINING

MANAGEMENT AUTHORISATIONS AND COMPLYING WITH OTHER ROBUST RISK STRATEGY REQUIREMENTS.5 CONSEQUENCES

4.1 Involvement in money laundering is a criminal offence, punishable by up to 14 years imprisonment. Not only the Council but also its officers and employees may face criminal prosecution if the Council is found to have been involved, even entirely innocently, in a deal involving the proceeds of a crime.

4.2 Therefore, it is important that all persons understand this policy and apply it at all times.

4.3 The remainder of this policy document sets out the law concerning money laundering and the rules you must follow to protect yourself and the Council from prosecution. The policy includes some technical information, but it has been drafted carefully to be as user-friendly as possible. Attached to the policy are copies of the documents you will need to become familiar with and complete for third parties with whom you engage in any transaction (or series of linked transactions) which involves cash or property worth approximately £13,000 or more or any other transaction which comes within the 'regulated sector'.

4.4 If there is anything you do not understand, please ask your manager or direct queries to the **MLRO**, Kevin Bartel, Interim Corporate Director of Resources (s151 officer).

5 THE RELEVANT LAW

5.1 The Proceeds of Crime Act 2002 (POCA)

5.1.1 This sets out the money laundering offences which apply generally to all UK citizens. These are;

(i) concealing, disguising, converting or transferring criminal property or removing criminal property from the UK (section 327);

(ii) entering into or becoming concerned in an arrangement which a person knows or suspects facilitates the acquisition, retention, use or control of criminal property (section 328);

(iii) acquiring, using or having possession of criminal property (section 329) (however, it is a defence to this charge if it can be shown that there were no grounds on which to suspect money laundering and the property was acquired for adequate consideration);

(iv) failing, in the case of the 'regulated sector'[1], to disclose knowledge or suspicion of money laundering to the **MLRO** or the failure by the **MLRO** (in the regulated sector and otherwise) to disclose such knowledge or suspicion to the National Crime Agency (**NCA** (sections 330, 331 and 332);

5.1.2 'Criminal property' means anything which is, or which represents, a direct or indirect benefit from any UK offence, no matter how minor.

5.1.3 If you are found guilty of any of the offences in paragraphs 5.1.1(i), 5.1.1(ii) or 5.1.1(iii) the maximum penalty on conviction in the Magistrates Court is up to 6 months imprisonment or a an unlimited fine or both a fine and imprisonment. The maximum penalty on summary conviction at the Crown Court is up to 14 years imprisonment or a fine or both a fine and imprisonment.

[1] Schedule 9, *The Proceeds of Crime Act (2002)* defines 'Regulated Sector' as including firms conducting business in the banking, financial and credit and insurance sectors, accountants, tax advisers and solicitors

5.1.4 If you are found guilty of any of the offences in paragraphs 5.1.1(iv) the maximum penalty on conviction in the Magistrates Court is up to 6 months imprisonment or an unlimited fine or both a fine and imprisonment. The maximum penalty on summary conviction at the Crown Court is up to 5 years imprisonment or a fine or both a fine and imprisonment.

5.1.5 As shown above, these offences are very broad in scope. If the Council or its officers or employees receive criminal property, even if in payment for an apparently legitimate commercial transaction, they may commit the offence of acquiring or having possession of it, and therefore be guilty of money laundering. However, you will have a defence if you make a formal written report in any case where you suspect money laundering (an authorised disclosure). All persons should make authorised disclosures internally, to the MLRO who can then decide whether to make a formal report to the authorities. Further details on how to make a disclosure are at section 10.

5.2 The Terrorism Act 2000

5.2.1 This Act establishes offences in relation to involvement in facilitating, raising, possessing or using funds for terrorism purposes that are similar to those under POCA. There are further parallels with POCA in relation to failing to report suspicious transactions. [2] HM Treasury maintains and updates a financial sanctions list which records individuals and organisations with whom it is prohibited to enter into any business relationship. The list can be viewed at http://www.hm-treasury.gov.uk/fin_sanctions_index.htm

5.2.2 As well as relying upon this list each person should consider whether there is a risk of terrorist financing in each transaction which takes place. This will involve considering the source and destination of funds.

[2] Sections 18-22, *The Terrorism Act (2000)*

5.4 The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (as amended) **("the 2017 Regulations) (as amended).**

5.41 These Regulations introduced significant changes to the anti-money laundering regime, such that regulated businesses are obliged to adopt a more risk- based approach towards AML, particularly regarding conducting due diligence and averting terrorist financing as follows:

(a) by extending the scope of due diligence checks, so that identity is fully checked. This includes a list of high-risk jurisdictions, which if involved in a transaction makes enhanced due diligence and additional risk assessments compulsory;

(b) introduction of enhanced due diligence, which includes extra checks to confirm identity, checking financial information, involving senior management with stricter ongoing monitoring of transactions and client relationships;

(c) enhanced restrictions on the reliance of a third party to carry out customer due diligence. Where an organisation relies on a third party, they are required to obtain copies of all documentation and ensure that there is a written agreement in place with the third party who must be compliant with the regulations;

(d) the introduction of Transparency of Ownership, so in addition to the UK Companies register, the regulations require a new Trust Register, requiring Trustees to register and report all Trusts that generate tax consequences;

(e) regulated business to apply stringent due diligence checks to business relationships with political exposed persons (PEPs), their family members and their known close associates,

(f) a requirement for regulated businesses to carry out an initial and periodic screening of relevant employees. This means an assessment of integrity, conduct, skills, knowledge and expertise of the individuals to carry out their functions effectively;

(g) introducing a new criminal offence: any individual who recklessly makes a statement in the context of money laundering which is false or misleading commits an offence punishable by a fine and/or up to 2 years imprisonment,

6 RELEVANT GUIDANCE – ASSESSING RISK

6.1 The Council has adopted a risk-based approach to anti-money laundering in accordance with guidance set down by the Joint Money Laundering Steering Group (available at www.jmlsg.org.uk). This recognises that most customers and contacts are not money launderers or terrorist financiers and that the systems and controls in place to combat the risk of money laundering should focus on identifying higher risk customers/contacts and situations and responding to them proportionately.

6.2 Generally, the Council's business will pose a low-to-moderate risk of being used as a vehicle for money laundering. It is involved in relatively few transactions (compared to say, a law firm, a bank or building society) and the nature of these is such that the participants are likely to come under scrutiny as to their bona fides, as well as their financial status. So opportunities for would-be money launderers to pass money through the Council with relative anonymity are limited.

6.3 Upon reviewing its risk profile, the senior management of the Council will update and approve a policy which embodies appropriate controls to manage and mitigate those risks. This is an iterative process. A minimum standard of identification will be required to facilitate this process. This is known as "simplified customer due diligence". Where a transaction or individual is considered to pose a higher risk, additional checks are required. This is known as "enhanced customer due diligence". See 7.2 for more details. If in doubt with regard to the level of risk in individual situations, you must seek advice from the **MLRO**.

7 CUSTOMER DUE DILIGENCE PROCEDURES

7.1 The legal requirement

7.1.1 The term 'Customer Due Diligence Measures' is derived from the 2017 Regulations [3] and used to describe the measures that need to be taken to obtain information including the customer's identity, the background to the customers business, the source of funds and the destinations of funds. The application of these measures should be reviewed regularly and in each transaction an analysis should be undertaken to consider the risk of money laundering or terrorist financing. The procedures below which are adopted by the policy set the minimum standards expected by the Council. Each person should be aware of the potential risks. Customer due diligence is more than just a box ticking exercise; it is each person's responsibility to risk assess each transaction.

7.1.2 Wherever the Council forms a business relationship, or carries out a one-off transaction involving a payment of €15,000 (currently approximately £13,400) or more, with an external individual or company (a 'customer'), it must obtain satisfactory evidence of identity. A business relationship is formed between the Council and another party where there is a business, professional or commercial relationship between them in relation to the provision of accountancy, audit or legal services, and where the Council expect, at the time when contact is established, that the relationship will have an element of duration. A one-off transaction is any transaction other than a transaction carried out during an established business relationship.

7.1.3 Council officers in other Service Areas who require accountancy, audit or legal services are internal customers and are not subject to the anti-money laundering provisions.

7.1.4 External customers to whom the Council may provide accountancy, audit or legal services include:

[3] Regulations 28 and where relevant regulation 29 and regulations 33-37 inclusive of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017

(a) Any person or body for which the Council has power, in exercise of its power to trade, to carry out or provide any services or work or provide any facilities or supplies under statutory powers, including under the well-being power.

(b) The bodies or organisations designated as "public bodies" for the purposes of the Local Authorities (Goods and Services) Act 1970.

(c) Partnership undertakings including the third sector.

7.1.5 The identity evidence must;

(a) Objectively viewed, be reasonably capable of establishing the identity of the individual or company, ("identification").

(b) In fact, establish to the satisfaction of the person who obtains it, that the person/company is who he/it claims to be ("verification").

7.1.6 **If such evidence of identity is not obtained the business relationship or the one-off transaction in question must not proceed any further.** The Regulations require the verification of identity as soon as reasonably practicable after the first contact. The Council's policy is that the requisite identification check(s) should take place within a minimum of **five working days** of the first business contact. If there is an unjustifiable delay in the evidence of identity being obtained from the customer or where the customer is deliberately failing to provide the information, a disclosure will have to be made.

7.1.7 Money laundering prevention is not simply a matter of box ticking, however. Remember that knowing enough about the people and businesses with whom we deal is just as important as confirming identity.

7.2 **The identification and verification process**

7.2.1 Identifying a customer is a two-part process. First, the individual or company is identified, by obtaining the following;

(a) Individual

(i) full name

(ii) current residential address

(iii) previous address if the customer has changed address in the last three months

(iv) date of birth

(v) nationality

(vi) country of residence

(vii) whether they constitute a Politically Exposed Person (further information as to what this means is set out in 8.4 below and Appendix A)

(b) Companies (most of the following should be available on their letterhead)

(i) full name of business

(ii) registered number

(iii) registered office

(iv) business address

(v) country of incorporation

(vi) (for private companies only) the names of all directors (or equivalent) and the names of all beneficial owners holding over 25% of the shares or voting rights.

(c) Trusts

(i) full name of the Trust

(ii) nature of trust (discretionary, bare, etc)

(iii) donor of the funds

(iv) nature of business or activity

(v) location of business or activity

(vi) country of establishment

(vii) names of all trustees

(viii) name of any protector or controller

(ix) names or classes of beneficiaries

(d) Charities (most of the following should be available from the Central Register of Charities)

(i) registered name

(ii) registration number

(iii) address of the Charity Commission's correspondent for the charity.

7.2.2 Second, the identification information should be **verified** using reliable, independent source documents, data or information. This may be produced by the customer or be obtained via electronic systems of identification (for example a credit reference bureau check).

7.2.3 There are several acceptable documents, which may be used to verify identity. These have been detailed on the Verification Checklists (**Appendix A)**, which include requirements for individuals and companies and other entities.

7.2.4 For face to face identification of individuals, production of a valid passport or photo card driving licence should be sufficient (simplified due diligence). However, if there are any unusual circumstances which would indicate a higher than normal risk (e.g. a foreign national, or a discrepancy in the details given and those recorded) then further checks will be required (enhanced due diligence).

7.2.5 For corporations, verification requires a search of the relevant company registry, a copy of the certificate of incorporation or confirmation of the company's listing on a regulated market. You must also take steps to be reasonably satisfied that the person you are dealing with is authorised to represent the company and is who he/she says they are. For private companies, it may be appropriate to verify the identity of one or more directors in accordance with the rules for identifying individuals. Verification may be limited to the individual giving instructions or someone who appears to be in active management or control of the company. Similarly, where the risk posed by a company is considered sufficient to warrant it, or the principal owner of a private company is another corporate entity or trust, it may be appropriate to verify the identity of beneficial owners.

7.2.6 Partnerships (including LLPs) and unincorporated businesses, if very well known, (e.g. law and accountancy firms) may be treated as publicly quoted companies (see 7.5.7(a)). Otherwise they may be verified by checking their regulated status by reference to membership of the relevant professional body (the Law Society or accountancy body). If neither of these is applicable, they should be treated as private companies.

7.2.7 Charities can take a number of legal forms. Some may be companies limited by guarantee, and should be treated as private companies. Other charities take the form of trusts. Details of registered charities are kept by the Charity Commission in a Central Register of Charities and information can be obtained from the website www.charity-commission.gov.uk or by ringing the enquiry line on 0845 3000218.

7.2.8 Churches are in general exempted by law from registering as charities and may not therefore have a registered number. Their identity can be verified by reference to the appropriate headquarters or regional organisation of the denomination.

7.2.9 The standard identification may be used for clubs and societies that serve a limited social or regional purpose. Following an assessment of the money laundering risk presented by the club or society, it may be appropriate to verify the identity of additional trustees (or equivalent).

7.2.10 In most cases simplified due diligence will be sufficient (see Appendix A). In circumstances which present a higher than normal risk of money laundering, however, either because of the nature of the customer or the transaction, or perhaps because the standard check gives rise to concern or uncertainty over identity, enhanced verification checks are likely to be appropriate, this is known as "enhanced customer due diligence" (see 8.3 for further information)

7.2.11 Banks and building societies are generally exempt from the verification requirements (see 8.5 below), and much less stringent requirements apply where the company is listed or is FSA regulated.

7.2.12 Unless otherwise specified, all documents examined should be originals and as recent as possible. Having inspected the original, you must take a copy for the Council's files. Always consider whether the documents provided appear genuine or may be forged. Where you are dealing with an agent, the identity and address of the actual principal should also be verified.

7.2.13 As well as obtaining satisfactory evidence of the identity and address, all persons must complete an appropriate Identity Verification Form (examples for individuals and for companies are at **Appendix B)**.

7.2.14 Once completed the Identity Verification Form must be sent to the MLRO to check compliance with the Regulations. Only once the MLRO has approved this and related documents, will identity be considered to have been verified. No money or property should be received or transferred before identity has been verified. Once verified the forms and supporting documents will be kept by the MLRO in a central file.

7.2.15 For future instructions/transactions, customers who have already been identified, where the Identity Verification Form is centrally filed, do not normally have to be identified again. However, where changes in their business set up have occurred, it may be necessary to do so (for example, if an individual has moved from one limited company to another).

7.2.16 In addition to the steps mentioned above, additional steps should be taken where appropriate to:

(a) establish the customer's circumstances and business, including, where appropriate, the customer's source of funds, and the purpose of specific transactions and the expected nature and level of those transactions;

(b) update information held on the customer to ensure the information held is valid;

(c) review information held on the customer to ensure it is current and valid; and

(d) monitor the customer's business activity and business transactions to ensure that the Council is not being used as a vehicle for money laundering.

7.3 **Enhanced customer due diligence**

In the circumstances outlined below and pursuant to regulation 33 of the 2017 Regulations, the Council will be required to apply enhanced customer due diligence measures and enhanced ongoing monitoring on a risk-sensitive basis.

7.3.1 **Non face to face transactions**

There is a greater likelihood of impersonation fraud and money laundering activity in non-face-to-face transactions. In most cases, this will warrant an additional verification check, which may involve seeing a separate document or, for example;

(a) requiring transactions to be carried out through an account in the person's name with a UK or an EU regulated credit institution;

(b) making telephone contact on a verified home or business land line; and

(c) communicating at an address which has been verified.

7.3.2 EDD - Red Flag Transactions

Changes to existing Enhanced Due Diligence (EDD) requirements mean that you must apply EDD in all the following circumstances (formerly it was only necessary if all the listed elements were met):

(a) where the transaction is complex;
(b) where the transaction is unusually large or

(c) where there is an unusual pattern of transactions, **or** the transaction or transactions have no apparent economic or legal purpose (formerly both conditions had to be satisfied).

(d) Whether a transaction is "complex" or "unusually large" should be judged in relation to the normal activity of the practice and the normal activity of the client.

7.4 Politically Exposed Persons (PEPS)

7.4.1 To determine whether the customer is a PEP, refer to Appendix A.

7.4.2 If the customer is a PEP it is necessary to:

(a) obtain approval from the MLRO to proceed with establishing a business relationship with such a customer;

(b) establish the source of wealth and source of funds which are involved in the business relationship or occasional transaction; and

(c) conduct enhanced ongoing monitoring of the business relationship.

7.4.3 High risk transactions/customers

7.4.3.1 High risk transactions or customers – if the customer or transaction appears high risk then further verification should be taken to verify the identity of that customer in order to ascertain whether the transaction is suspicious and whether disclosure is to be made. Further documentation which may be required is listed in Appendix B. In addition the source of the funds to be transferred should be ascertained

7.5 Ongoing monitoring

7.5.1 It is the duty of the Council to monitor transactions or customers and to assess each transaction with respect to the risk it poses of money laundering activity or terrorist financing.[4]

[4] Regulation 40, The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017

7.5.2 Each employee should assess each transaction as to its complexity, suspiciousness, and legal purpose as well as the magnitude, sums, frequency of transactions or any other special characteristics to ensure that they correspond with regular activities of that particular customer.

7.5.3 The documents, data or information obtained by the Council for the purpose of applying customer due diligence measures must be kept up to date.

Exemptions from the identification process

7.5.4 The identification and record keeping requirements do not apply in respect of any one-off transaction where payment is to be made by or to an individual or company of less than €15,000 or in respect of two or more linked one-off transactions, the total amount in respect of which is less than €15,000 and where there is no suspicion of money laundering.[5] In the absence of evidence to the contrary, transactions which are separated by an interval of six months or more need not be treated as linked.

7.5.5 Financial institutions regulated by the FSA, or in the EU or comparable jurisdiction by an equivalent regulator, do not need to be verified. This will encompass banks and building societies. However, for smaller firms, if there is any doubt as to their regulated status, this should be checked before proceeding without verification (www.fsa.gov.uk).

7.5.6 Where a one-off transaction is carried out (but not where there is a business relationship) pursuant to an introduction effected by an FSA-regulated firm or individual, and that firm or individual has provided written assurance that satisfactory evidence of individual identity of the contact introduced by him has been obtained and recorded, evidence of identity is not required.

7.5.7 Where the customer is;

(a) a publicly quoted company

(b) a majority-owned and consolidated subsidiary of a publicly quoted company

(c) subject to the licensing and prudential regulatory regime of a statutory regulator (e.g. OFGEM, OFWAT, OFCOM)

nothing is required beyond the standard identification.

[5] Regulation 27(2), 2017 Regulations

7.5.8 It is important to note that **the above exemptions only apply where there is no suspicion of money laundering**. So even if you are dealing with a bank, or have written assurance from another regulated service provider in the financial services sector that it has obtained satisfactory evidence of identity - if you still have a suspicion you have to undertake the checks and make a disclosure to the MLRO.

8 INFORMATION MANAGEMENT ISSUES

8.1 Data Protection

8.1.1 Under the Data Protection Act 2018 (**the 2018 Act**) and the General Data Protection Regulation 2016 (as amended) (**the GDPR**) an external customer may request in writing:[6]

(a) a copy of all the personal data of which that person is the data subject and any information available to the Council on the source of that data; and

(b) information on the processing of any personal data by the Council, a description of that data, the purpose for which the data are being processed and to whom the personal data has or may be disclosed

(c) members of the public can also seek to find out how their data is being used, have incorrect data updated, have data erased and also to object to how their data is processed in certain circumstances.

8.1.2 The Council must respond to a request for information promptly and in any event not more than one month from the date on which the request is received.

8.1.3 The 2018 Act contains certain exemptions from the right of access to personal data. One such exemption is where the right of access would be likely to prejudice the prevention or detection of crime or apprehension or prosecution of offenders.[7]

8.1.4 The exemption from the right of access to personal data will apply where the disclosure of personal data would result in the commission of the tipping-off offence under POCA.[8]

8.1.5 The exemption is not automatic and each case should be considered on its merits to ensure that the exemption applies. Always take advice from the MLRO.

---

[6] Article 15, GDPR
[7] Schedule 2, part 1 of the Data Protection Act 2018
[8] Schedule 1, part 2 of the Data Protection Act 2018

8.1.6 The Council's Data Protection Policy can be viewed on the Council's intranet, http://www.towerhamlets.gov.uk/data/your-council/data/data-protection-act.cfm and in the Council's Data Protection Manual. Guidance on the application of the policy and the 2018 Act can be obtained from the Council's Data Protection Officer, Darren Thomas.

8.2 Freedom of Information

8.2.1 The Freedom of Information Act 2000 (the 2000 Act) gives members of the public a general right of access to all types of recorded information held by public authorities, which includes the Council. The general right of access is however subject to exemptions.

8.2.2 Information held by a public authority is exempt information:

(a) if it was directly or indirectly supplied to a public authority by, or relates to various government bodies, which includes NCA (section 23);

(b) if its disclosure would, or would be likely to, prejudice the prevention or detection of crime or apprehension or prosecution of offenders (section 31).

8.2.3 These exemptions should not be applied without taking advice from the MLRO.

8.2.4 Details on Freedom of Information can be viewed on the Council's Intranet at http://www.towerhamlets.gov.uk/data/your-council/data/foi/index.cfm

8.2.5 Details about the how the Council manages records can be found in the Council's Information Management and Governance Policy.

8.2.6 Advice about Freedom of Information can be obtained from the Information Governance Manager.

9 MAKING A DISCLOSURE

9.1 How to make an authorised disclosure – internal reporting procedures

9.1.1 If you are involved in any transaction – for example the sale or purchase of shares or property - where you either know or suspect that the money or property concerned is the proceeds of any crime, you risk being found personally guilty of money laundering unless you make an **authorised disclosure.** This is a disclosure, in the prescribed form, to the designated Money Laundering Reporting Officer (MLRO), Kevin Bartel, Interim Corporate Director of Resources (s151 officer) . It must be made as soon as is reasonably practicable; i.e. within hours of the relevant information coming to your attention, or the very next day at the latest. What is likely to constitute suspicion is dealt with in section 13.

9.1.2 Where any person is aware of, or has reason to suspect, money laundering, they must complete a Money Laundering Disclosure Form (**Disclosure Form)** indicating the reason for their suspicions. Please see **Appendix C** for a pro-forma of this form and detailed guidance on how to complete it. A copy of the relevant Identity Verification Form should be attached to this form and both documents forwarded to the MLRO. In no circumstances should a copy of the Disclosure Form be put on the file or otherwise disclosed to anyone other than the MLRO.

9.2 The Council requires all disclosures be made to the MLRO, Kevin Bartel, Interim Corporate Director of Resources (s151 officer) **, whose contact details are:**

Internal extension: 020 7364 4915

External Telephone Number: 020 7364 5000

Email:
kevin.bartel@towerhamlets.gov.uk

9.2.1 If Kevin Bartle is not available at the time you want to make a disclosure, the disclosure should be made to the MLRO's Deputy, Paul Rock, Head of Internal Audit, Anti-Fraud & Risk, telephone 07562 431830.

9.2.2 The MLRO will acknowledge receipt and decide whether it is appropriate to make a formal disclosure, known as a Suspicious Activity Report (**SAR**), to one of the external authorities mentioned.

9.2.3 Please note that it does not matter whether the suspected crimes, or the proceeds of it, are extremely minor. The law is very strict – everything must be reported.

9.3 **The offence of failing to disclose**

9.3.1 If you;

(a) know or;

(b) suspect or;

(c) have **reasonable grounds** for knowing or suspecting

that another person is engaged in money laundering, you commit an offence if you do not disclose it to the MLRO as soon as practicable after you receive the information (POCA section 330).

9.3.2 It is important to note that this is an objective test. Even if you genuinely do not know or suspect that someone is engaged in money laundering, you may commit an offence if there are reasonable grounds for knowing or suspecting money laundering. So if you deliberately shut your mind to the obvious, you may be culpable. To protect yourself, you must think very carefully whether, in any given transaction, there is anything slightly odd or 'iffy'. If so, you must make a disclosure to the MLRO. Please read section 133 below, which will give you some pointers as to behaviour or circumstances which may appear unusual. Whilst this clearly cannot be exhaustive, as no two situations are identical, it should help you develop an enquiring approach.

9.3.3 If the disclosure is made after the prohibited act, the disclosure defence will not apply unless there is a reasonable excuse for not having disclosed in advance.

9.3.4 If the MLRO receives a disclosure report on the basis of which he knows or suspects, or has reasonable grounds for knowing or suspecting, that someone is engaged in money laundering, he commits an offence if he fails to disclose it as soon as possible to NCA.

9.3.5 The failure to report offences are punishable by up to 5 years imprisonment.

9.4 **The role of the MLRO**

9.4.1 Upon receipt of a Disclosure Form, the MLRO must note the date of receipt on his section of the report and acknowledge receipt of it.[9] He should also advise you of the timescale within which he expects to respond to you.

9.4.2 The MLRO will then consider the report and any other relevant information to decide whether the information gives rise to a knowledge or suspicion of money laundering.[10] Relevant information will include;

(a) reviewing other transaction patterns and volumes;

(b) the length of any business relationship involved;

(c) the number of any one-off transactions and linked one-off transactions; and

(d) any identification evidence held.

9.4.3 The MLRO must undertake such other reasonable inquiries he thinks appropriate in order to ensure that all available information is taken into account in deciding whether a report to NCA is required (such enquiries being made in such a way as to avoid any appearance of tipping off those involved).

9.4.4 The MLRO may also need to discuss the report with you. All persons are required to cooperate with the MLRO and the authorities during any subsequent investigation.

9.4.5 Once the MLRO has evaluated the Disclosure Form and any other relevant information, he must make a timely determination as to whether:

(a) there is actual or suspected money laundering taking place; or

(b) there are reasonable grounds to know or suspect that is the case; and

[9] Regulations 18-24 of the 2017 Regulations, see in particular Regulation 18(4).
[10] Regulation 21(5) of the 2017 Regulations.

(c) whether he needs to seek consent from NCA for a transaction to proceed.

The decision must be recorded on part two of the Disclosure Form.

9.4.6 If the MLRO decides that the information does give rise to a suspicion of money laundering, he is required to make a SAR to the law enforcement authorities as soon as practicable, unless he has a reasonable excuse for non-disclosure. If he concludes that such a reasonable excuse exists (after taking legal advice if appropriate), the MLRO must mark the report accordingly before giving his consent for any ongoing or imminent transactions to proceed.

9.4.7 Any material which it is concluded should be disclosed may be subject to legal privilege. Please refer to section 11 below.

9.4.8 If there is no reasonable excuse for not reporting to NCA, the MLRO must make his report on the standard report form and submit it in hard copy or electronically in accordance with the procedure set out on the NCA website (www.NCA.gov.uk). This website also includes helpful guidance for MLROs on how to complete an SAR.

9.4.9 To submit electronic reports, the Council must first be registered with the SAR online reporting facility https://www.ukciu.gov.uk/(thullbfm04gadsru25x3tn45)/Information/info.aspx?InfoSection=Submission

9.4.10 In the absence of a reasonable excuse for not reporting to the authorities, the MLRO commits a criminal offence if he knows or suspects, or has reasonable grounds to do so, (because of a disclosure made to him), that another person is engaged in money laundering and he does not disclose this as soon as practicable to NCA.

9.4.11 Once a report has been made, no further action should be taken about the matter until it is expressly or impliedly permitted by NCA (see 11.2 below).

10 LEGAL PROFESSIONAL PRIVILEGE

10.1 Solicitors and all other legal staff and legal services' support staff will be handling material subject to legal professional privilege. There are two categories of legal professional privilege; legal advice privilege and litigation privilege.

10.2 The broad outline of the type of communication which attract privilege are set out below. The existence of legal privilege may affect the basis of a money laundering disclosure. Always take evidence from the MLRO if you believe privilege attaches to relevant information.

10.3 **Legal Advice Privilege**

10.3.1 Legal advice privilege applies to;

(a) confidential communications;

(b) which pass between members of the Council or other council staff and solicitors and other legal services' staff; and

(c) which have come into existence for the purpose of obtaining legal advice in relation to the business of the Council.

10.3.2 Confidential communications are limited to those that directly seek or provide legal advice. Communications which merely pass information between legal services' staff to members of the Council or other council staff **should not contain legal advice** as this could lead to loss of privilege to the whole document.

10.3.3 Legal advice privilege does not attach to communications prepared for the purpose of or which form part of a criminal act, or to communications seeking legal advice for the purpose of furthering a criminal act, even if the legal adviser is not aware of the true purpose of preparing the documents or seeking legal advice. Consequently, documents and communications known to have been made for the purpose of furthering money laundering do not benefit from legal advice privilege.

10.3.4 Where there is only a suspicion of money laundering and the documents involved are subject to privilege, section 338 of POCA 2002 provides that an "authorised disclosure" may be made without breaching legal privilege.

10.4 Litigation Privilege

10.4.1 Ligation privilege applies to;

(a) confidential communications when litigation is pending or contemplated;

(b) which pass between members of the Council or other council staff and solicitors and other legal services' staff; and

(c) which pass between the council's solicitors or legal services' staff and the solicitors or legal advisers of the other party or parties to the proceedings.

10.4.2 A solicitor or legal adviser may be in contempt of court if he discloses information to NCA that is protected by litigation privilege.

10.5 Checks for Lawyers

(a) Consider any unusual transactions and do appropriate due diligence particularly in relation to source of funds;

(b) Carry out enhanced verification checks in relation to identity, property, trusts, monetary activity as a minimum;

(c) Seek to understand the rationale for any litigation/business transactions;

(d) Document any transactions and adopt a risk- based approach;

(e) Monitor ongoing business/client relationships;

(f) Ensure transactions are appropriate for the instructions;

(g) Review existing records and consider the reasoning for every transaction/contract;

(h) Consider whether there is the possibility of sham litigation and/or suspicious instructions.

11 AFTER A DISCLOSURE HAS BEEN MADE

11.1 Caution

11.1.1 Once you have made a disclosure to the MLRO, you must not discuss the matter with anyone else and you must not do anything further in connection with the deal or transaction until you receive direct instructions from the MLRO. You must not make further enquiries into the matter yourself; any necessary investigations will be undertaken by the MLRO, or NCA, in the event that the MLRO decides to make an SAR.

11.1.2 If the MLRO determines that it is appropriate to make an SAR to NCA, you cannot proceed without NCA's consent. More details on the procedure for obtaining consent and what you must do in the meantime are outlined at section 11.2.

11.2 Consent

11.2.1 If the MLRO decides that your report does not require onward reporting to NCA, he will give you consent to proceed.

11.2.2 Once a disclosure had been made to NCA, the Council must do nothing further in connection with the particular transaction giving rise to the suspicion. If nothing is heard from NCA after 7 working days, then consent is deemed to have been given for the transaction to proceed. If, however, NCA responds within 7 working days with a request for more time, then the 31 day moratorium period will take effect. During this period, the transaction must not proceed unless and until either consent is received or the 31 day period expires. If NCA does not respond within that time, the Council can conclude that implied consent has been granted for the transaction to proceed.

11.2.3 The authorities can apply for a restraining order before the end of the moratorium period if they wish to stop the transaction going ahead at all.

11.2.4 These time limits must be strictly adhered to. It may be that at some later date the Council may by court order be ordered to produce documentation.

12 TIPPING OFF

12.1 At no time and under no circumstances should you voice any suspicions to the person(s) whom you suspect of money laundering, even if NCA has given consent to a particular transaction proceeding. This amounts to 'tipping off' and is an offence under POCA, section 333A. A person commits this offence if, knowing or suspecting that an authorised or protected disclosure has been made, he makes a disclosure (whether to the suspect or any third party) which is likely to, and which he knows or suspects is likely to, prejudice any investigation. The maximum penalty is five years in prison.

12.2 It is vital that you do not discuss details about a disclosure with anyone where it might prejudice any investigation. Clearly, the individual or company who is the subject of the report cannot be informed. Nor can anyone else who may inform them. The safest position is to limit discussions about suspicion and disclosure with the MLRO.

13 WHAT IS SUSPICIOUS?

13.1 Suspicion is less than knowledge, but more than mere speculation or gossip. It must be built on some foundation. A transaction which appears unusual will not necessarily be suspicious. 'Unusual' is, in the first instance, a basis for further enquiry, which may in turn require judgement as to whether it is suspicious. It is impossible to give an exhaustive list of circumstances and activities which will trigger suspicion. Sometimes it may be a combination of factors which individually would not give cause for concern. However, in the context of the Council's business, the following are common examples which may, depending on the particular circumstances, be likely to trigger suspicion:

13.1.1 Secretive individuals or companies. Be particularly cautious if you don't meet people in person, or if there is any attempt to conceal identity, for example, via the use of post office boxes.

13.1.2 Unusual arrangements, for example complex company structures or trusts with no apparent commercial purpose or companies with nominee directors.

13.1.3 Receipt of, or a request for payment in, substantial sums of cash (over €15,000).

13.1.4 Any request to hold sealed boxes/parcels.

13.1.5 Unusual Settlements by cash or bearer cheques of any large transactions involving the purchase of property or other investments.

13.1.6 A deal which is uncommercial for one or more participants; launderers are prepared to lose a high percentage of the initial funds, just to 'wash' large sums of cash.

13.1.7 Overpayments by any party.

13.1.8 A transaction is proposed but the person you are dealing with is not the person behind the deal/company and you do not meet this person.

13.1.9 Illogical third party transactions, for example unnecessary routing or receipt of funds from third parties or via third party accounts.

13.1.10 Payment by way of third party cheque or money transfer, where there is a variation between the account holder, the signatory and a prospective investor.

13.1.11 Funds for deposits or completion on a property transaction which come from an unexpected source; alternatively where instructions are given for settlement funds to be paid to an unusual destination.

13.1.12 Any other involvement of an unconnected third party without logical reason or explanation.

13.1.13 An abortive transaction which has fallen through for no good reason.

13.1.14 Radical changes/developments to an original proposition for no discernible reason.

13.1.15 Poor business records and internal accounting controls.

13.1.16 Proof of identity documents which don't look or feel quite right.

13.1.17 A transaction which is unusually large, or small.

13.1.18 An unusual deal/contact either in terms of size or location.

13.1.19 Any matter having a link with countries where production of drugs or drug trafficking may be prevalent. The Financial Action Task Force (FATF) publishes a list of non co-operative countries and territories annually (go to www.fatf-gafi.org).

13.1.20 Fellow employees whose lifestyle indicates an income in excess of position/salary or whose level of performance falls. Money launderers have been known to 'buy off' or blackmail staff whom they have enticed into drug use to turn a blind eye to laundering transactions.

13.1.21 Funds being received from, or going to, an offshore location may be a possible indicator that money coming into or being paid out on a transaction is not being declared properly for tax.

13.1.22 Transactions significantly above or below market price or which appear uneconomic inefficient or irrational.

13.1.23 Anything which seems too good to be true.

13.2 It is important to think laterally. Be alert to transactions which could constitute money laundering, even though they may not fall within the common perception of money laundering, i.e. receiving the proceeds of drugs trafficking or a bank robbery.

14 RECORD KEEPING PROCEDURES

14.1 All disclosure reports referred to the MLRO and reports made by him to NCA must be retained by the MLRO in a confidential file kept for that purpose for a minimum of five years.[11] The Regulations require that the Identity Verification Form and the record of transactions (the transaction file and other relevant records) be retained for at least five years from:

14.1.1 in the case of the Identity Verification Form and related evidence, the date the business relationship ends or the date of completion of all activities taking place in the course of the one-off transaction or the last one-off transaction where linked; and

14.1.2 in the case of the record of transactions, the dates on which all activities taking place in the course of the transaction were completed.

14.2 However, for cases where a report to NCA is made, the relevant records must not be destroyed without reference first to NCA. It is the responsibility of the MLRO to ensure that such records are retained after their normal five year retention period.

[11] See Regulations 21(8) and 40.

15 TRAINING

15.1 The Regulations require that key staff involved in relevant business and any clerical, secretarial, administrative or accounts staff assisting them, be provided with adequate training to ensure they are aware of, and understand, their legal and regulatory responsibilities and their role in implementing the Council's internal procedures.[12] This is to be co-ordinated by the MLRO.

15.2 In the event that any person is contacted by NCA, the police, HM Revenue and Customs or any other law enforcement body with regard to a money laundering matter, they should refer the enquiring party to the MLRO in the first instance, who will obtain details of their requirements and decide how to proceed.

[12] Regulation 24 of the 2017 Regulations.

16 SUMMARY OF RESPONSIBILITIES

16.1 **Key Officers must:**

16.1.1 Read and follow this policy.

16.1.2 Know and understand the legislation.

16.1.3 Take reasonable steps in accordance with procedures to identify and verify the identity of any person or company with whom it is proposed to deal.

16.1.4 Remain vigilant at all times and alert to suspicions.

16.1.5 Report any suspicions to the Money Laundering Reporting Officer (MLRO) in accordance with internal procedures.

16.1.6 Complete the multimedia training programme and pass the test to reinforce understanding of the law, internal rules and procedures.

16.1.7 Keep appropriate records for at least five years, and indefinitely in cases where an SAR has been made.

16.2 **The MLRO must;**

16.2.1 Monitor compliance.

16.2.2 Ensure that policy and procedures are developed and maintained in accordance with evolving statutory and regulatory obligations and guidance.

16.2.3 Review the policy and the Councils' general assessment of risk, at least annually, to determine whether changes are appropriate.

16.2.4 Ensure that training is offered and that the standards and scope of training are appropriate and necessary records are kept.

16.2.5 Report to senior management as appropriate on money laundering compliance matters.

16.2.6 Consider all internal disclosures and make Suspicious Activity Reports (SAR) to the National Crime Agency (NCA) as appropriate.

16.2.7 Ensure that records are kept for the requisite five years, or indefinitely in cases where an SAR has been made.

APPENDIX A

CUSTOMER IDENTIFICATION –
VERIFICATION CHECKLIST OF
ACCEPTABLE SOURCES OF INFORMATION

CUSTOMER IDENTIFICATION NOTES PLEASE READ IN CONJUNCTION WITH VERIFICATION CHECKLISTS

1 DOCUMENT REQUIREMENTS AND CERTIFICATION

All documents must be original and as recent as possible. A copy should be retained and noted as to who saw the original and when. Only the personal detail pages of a passport need to be copied – in black and white – and retained.

If you are satisfied that there is a good reason why you cannot meet the customer and see original documentation, copies certificated as set out below may be relied on.

(a) UK residents

- Passports;

  - UK notaries, solicitors whose name and address should be noted and checked against the Law Society database of practising solicitors, government departments and British consulates

  - Financial institutions and other persons and firms subject to the 2017 Regulations.

- Other documentary evidence;

  - For example by a UK solicitor, doctor or high street bank manager, whose name and address should be noted and checked by reference to a professional directory or, for solicitors, as above**.**

(b) Non–UK Residents

Copy documentary evidence can be certified by;

- An embassy, consulate or high commission of the country of issue;

- A qualified lawyer or notary, verifying his/her name and practice address in a reputable professional directory, or that the professional is currently on record with the appropriate professional body as practising at the address shown on the certificate or practice notepaper, keeping a note

of this name and address with the evidence of identity.

1. Politically Exposed Persons

2.1 These are individuals who are or have been entrusted with prominent public functions including:

- Heads of state, heads of government, ministers, and deputy or assistant ministers;
- Members of parliament;
- Members of supreme courts, constitutional courts or other high-level judicial persons
- Members of courts of auditors or of the boards of central banks
- Ambassadors and high-ranking officers in the armed forces;
- Members of the administrative, management or supervisory bodies of State-owned enterprises.

and

- Are resident outside the United Kingdom
- Are or have, at any time in the preceding year been entrusted with a prominent public function by a state other than the United Kingdom or by the Community or by an international body.

2.2 Individuals who are immediate family members, of a person listed in 2.1 above, which includes

- a spouse;
- a partner;
- children and their spouses or partners; and
- parents.

2.3 Individuals who are known close associates, of a person listed in 2.1 above, which includes:

- any individual who is known to have a joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations with a person in 2.1 above.
- any individual who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of the person in 2.1 above.

3. Overseas Corporations

Where the Customer is a non-UK company comparable documents to those for a UK company should be obtained and similarly one director or shareholder should be identified as set out for a UK company. Care should be taken to verify the legal existence of the company and to ensure that any person purporting to act on behalf of the company is so authorised. It is important to look behind the corporate identity to establish who has ultimate control.

4. Principal and agent relationships

Where the customer is not acting as the principal but as agent then the identity and address of the actual principal should also be verified.

PART I

PRIVATE INDIVIDUALS OR DIRECTORS/PARTNERS OF CORPORATE BODIES

Standard Verification of Identity

STEP ONE

Ask the individual to confirm their full name, current residential address (and previous address if it has changed in the last three months), date of birth, nationality and country of residence.

STEP TWO

Verify the information based on documents produced by the individual or electronically (e.g. via a credit reference bureau)

1. **Face-to-face dealings**

   Choose either:

   - **One item from LIST A or**
   - **One item from LIST B and one item from LIST C**

   and record the details as prescribed.

2. **Non face-to face dealings**

   As 1. above, but consider whether an additional verification check is required; either an additional piece of information, an electronic verification or another measure, for example:

   - a) Requiring any financial transaction to be effected via an account in the individual's name with a UK or EU regulated institution

   - b) Making telephone contact via a verified home or business land line

   - c) Communicating with the individual at an address which has been verified

   - d) Requiring any copy documents to be certified by an appropriate person.

Non-standard verification of identity

Where an individual or a transaction is considered higher risk, the standard verification procedure may be inadequate. This may arise, for example, where completion of the standard verification check has given rise to concerns. In such cases, the number of matches required to be reasonably satisfied as to as to the individual's identity will increase. If in doubt, seek advice from the MLRO as to what is required in non-standard cases.

LIST A

Government issued photographic ID with full name and address or DOB

	IDENTIFICATION DOCUMENTS	**DETAILS TO BE RECORDED**
1	**Valid full UK/EC signed Passport**	**Name** **Passport Number** **Country of Issue** **Date of Issue** **Date of Birth**
2	**Current UK or EEA photo-card driving licence (full or provisional)**	**Name** **Licence Number** **Address** **Date of Birth** **Valid From and Valid to dates**
3	**National identity card containing a photograph (non-UK nationals only)**	**Names** **Number** **Country of Issue** **Date of Issue** **Date of Birth**
4	**Firearms certificate or Shotgun licence**	**Name** **Number** **Date** **Valid Until**
5	**Identity card issued by the electoral office for Northern Ireland**	**Name** **Number** **Date of issue** **Date of birth**

LIST B

Government-issued documents (without a photograph) which show the individual's full name

	IDENTIFICATION DOCUMENTS	DETAILS TO BE RECORDED
1	Valid (old style) full UK driving licence	Name Number Date of issue Valid until
2	Housing benefit, council tax benefit or state pension statement	Name Number Date
3	Inland Revenue Self-Assessment Statement or Tax Demand (current tax year only)	Tax Reference Number Date of Issue Name of Issuing Tax Office
4	Tax demand or statement	Name NI number Reference number Date

5	**Armed Forces Identity Cards**	**Name** **Services Number** **Rank Held**

LIST C

EITHER - a document issued by government, a judicial authority, public sector body or an FSA (or comparable) regulated firm which must incorporate the individual's full name and his residential address or his date of birth

OR - confirmation of a visit to the home address

1	**Recent Utilities Bill or Statement not more than 3 months old (inc telephone, gas, water rates and electricity) - or similarly recent Certificate from a Utilities Supplier confirming an arrangement to pay for services on pre-payment terms** **Do not accept mobile phone bills or utility bills printed off the internet**	**Customer Account Number** **Name of Utility** **Date of Bill**
2	**Council Tax Bill or statement** **Not more than 12 months old**	**Property Reference Number** **Name of Issuing Local Authority** **Date of Bill**
3	**Bank, Building Society, Credit Union Statement or original Mortgage Statement from a regulated financial sector firm in the UK, EU or comparable jurisdiction (not more than 12 months old or printed off the internet) or passbook containing current address**	**Account Number** **Account Name** **Name of Bank or Lender** **Date of Statement** **Date of last entry in passbook**

5	**Medical Card**	**National Health Service Number** **Date of Birth** **Name of Issuing Authority**
6	**Current house or motor Insurance Certificate**	**Insurance Company** **Policy Number** **Date**
7	**Visit to customer's home address**	**Details**

Part II –CORPORATE BODIES AND OTHER NON-PERSONAL ENTITIES

(N.B for the purposes of ID verification, partnerships (including LLPs) and unincorporated businesses, if very well known, (e.g. law and accountancy firms) may be treated as publicly listed companies. Otherwise they may be verified by checking their regulated status by reference to membership of the relevant professional body (law society or accountancy body). If neither of these is applicable, they should be treated as private companies.)

Standard Verification of Identity

STEP ONE

Obtain full name, registered number, registered office and business address (should be on letterhead/notepaper)

For private companies only, also obtain names of all directors (or equivalent) and names of beneficial owners holding over 25%

STEP TWO

Verify the information

- **If you are satisfied the company is listed, or a subsidiary of a listed company, or is regulated by the FSA or equivalent (i.e. a bank or building society) or OFGEM, OFWAT or OFCOM, you need take no further action. This status may be self-evident, but for smaller or less well know companies, double check via the appropriate website.**
- **Otherwise, you should undertake a search of the relevant company registry or obtain a copy of the certificate of incorporation and record;**

  - Company Number
  - Registered Office Address
  - Directors Names and addresses
  - Shareholders names and addresses

<u>Non-standard verification of identity</u>

The standard evidence is likely to be sufficient for most corporate entities. If, however, a higher risk is presented, additional evidence may be required. Higher risk indicators may include entities which are;

- **smaller**
- **opaque**
- **lacking industry profile**
- **based in less transparent jurisdictions**
- **associated with a high risk territory or a politically exposed person (PEP) or**
- **where the standard verification process has thrown up something unusual.**

Additional evidence may include verification of the identity of one or more directors or beneficial owners with a holding of over 25% (in accordance with the individual verification checklists). Special care must be taken in respect of any company with bearer shares, which make it difficult to identify the beneficial owners. In such cases, a written undertaking must be obtained from the beneficial owner that they will provide immediate notification in the event of a transfer of shares to another party.

APPENDIX B

IDENTITY VERIFICATION FORMS

IDENTITY VERIFICATION FORM

PART I - PRIVATE INDIVIDUAL

Please refer to verification checklists A, B and C and related notes in completing this form

1	**Name (including aliases)**	
2	**Address (including post code)**	
3	**Telephone No (including area code)**	
4	**Fax No (including area code)**	
5	**E-mail address**	
6	**Date of first contact (DD/M/YY)**	
7	**Summary of transaction and party's involvement in it**	

8	**Acting as principal?** **(If no, identify principal on a separate form)**	**YES/NO**
9	**Standard verification of customer's identity** **- Government issued photo ID (verification list A)** **OR** **- government issued non-photo ID showing full name (list B)** **AND** **- document issued by government, judicial authority, public sector body or FSA regulated firm, showing address or DOB/home visit (list C)** **Document(s) Checked?** **Relevant details recorded? (LIST**	

	name, address, DOB, document issuer, reference/account numbers, issue date, valid from and valid to dates as appropriate) **Any other Relevant Details**	
10	**Evidence of identity attached?** **If no, give reason; if yes specify**	**YES/NO**
11	**Face-to-face contact?** **If no, what additional steps have been taken to verify identify?** **- telephone/ postal contact to verified land line number/residential or business address?** **- Certified documents?** **- Electronic verification?**	**YES/NO**
12	**Is the customer a Politically Exposed Person? (Refer to paragraph 2 of Appendix A above)** **Is the customer an individual who has held a prominent public position or an immediate family member or a known close associate of such an**	**YES/NO**

	individual? **Resident outside the United Kingdom?** **At any time in the preceding year carried out a prominent public function for a state other than the UK, or for the Community, or for an international body?** **If yes to any of the above this must be referred to the MLRO for approval**	**YES/NO** **YES/NO**
13	**Non-standard verification required? (for higher risk customer/transaction)** **If yes give details of additional verification undertaken**	**YES/NO**
14	**Evidence of identity satisfactory?**	

15	**Signature and Reference** **Date**	**……...** Ref ……
16	**Signature and reference of MLRO**	**……...** Ref ……
17	**Date business relationship/one-off transaction completed:**	
18	**Record destruction date (5 years from the date in 16)**	

Note: This record must not be destroyed at the date of destruction if a report has been made to the Serious and Organised Crime Agency (NCA) without reference first to NCA.

Notes:

1 Copies of the evidence of identity and address must be attached.

2 This form and supporting documents must be sent to the MLRO for filing.

IDENTITY VERIFICATION FORM

PART II - CORPORATE AND OTHER ENTITIES

1	**Name (including trading names)**	
2	**Type of legal entity (corporate, trust, etc)**	
3	**Registered number (corporates)**	
4	**Registered and business/location address (including post code):**	
5	**Telephone Number (including area code):**	
6	**Fax Number (including area code)**	
7	**E-mail address**	
8	**Country of incorporation**	

9	**Type of business**	
10	**Regulatory body**	
11	**Contact Director/Shareholder (Minimum of one name)**	
12	**Names of principal beneficial owners (over 25%)**	
13	**Date of first contact (DD/MM/YY)**	
14	**Summary of transaction and role of party**	
15	**Acting as principal? (If no, identify principal on a separate form)**	**YES/NO**
16	**Exemption from verification procedure** **a) Is the Company (or its parent) a UK/EU bank or a building society, or**	 **YES/NO**

	otherwise FSA regulated? (if in doubt check the on-line FSA register (www.fsa.gov.uk) showing that authorisation by the FSA to carry on relevant business)	
	b) Is the company listed or its shares or securities traded on any other recognised, designated or approved exchange or subsidiaries (check if necessary via www.fsa.gov.uk)	**YES/NO**
	c) Is the company a subsidiary of a company under b)? (If necessary, obtain evidence of listing of parent and of relationship to parent such as a copy of the latest annual return or extract from a reputable on-line provider).	**YES/NO**
	d) Is the company OFGEM, OFWAT or OFCOM regulated?	**YES/NO**
	e) Is it a well known accountancy or law firm? (if not sure, check details with the Law Society or relevant accountancy body)	**YES/NO**
	(if YES to any of above, give details and proceed to question 20)	

17	**Verification of identity - private companies** **Search of Companies House Register and or certificate of incorporation and record;** **- company name** **- company number** **- registered address** **- directors names and addresses** **- shareholders names and addresses** **- names of beneficial owners holding over 25%**	
18	**Verification of identity – other bodies;** **a) NHS Trusts – evidence from Department of Health website, a certificate copy of the relevant resolution and evidence that the instructing representative is duly authorised.** **b) Local authorities – evidence from Directory of Local Authorities, a certificated copy of the relevant resolution and evidence that the instructing representative is duly authorised.** **c) Educational institutions – extract from relevant charter or Act and SI, showing creation and powers and evidence that the instructing representative is duly authorised.** **d) Partnerships and limited**	**Record relevant details**

	partnerships – evidence of identity of partner instructing and one other partner, with satisfactory evidence of trading address (possibly from a directory or similar).	
19	**Non-standard verification required? (where higher risk indicators exist, e.g. smaller, opaque businesses, based overseas, involving politically exposed persons)** **If yes give details of additional verification undertaken (for example, separate individual identity verification for individual director(s) or shareholder(s)**	**YES/NO**
20	**Evidence of identity attached?** **(If no, give reason)**	**YES/ NO**
21	**Evidence of identity satisfactory? (If no, please explain)**	**YES/NO**

22	**Signature and reference**	…….. Ref ……
23	**Signature and reference of MLRO** **Date**	…… Ref …….. ……../……./…….
24	**Date business relationship/one-off transaction completed**	……./……./…….
25	**Record destruction date** **(5 years from the date in 18)**	……/……/……

Note This record must not be destroyed at the date of destruction if a report has been made to the Serious and Organised Crime Agency (NCA) without reference first to NCA.

Notes:

1 'Corporate' bodies include listed and unlisted companies and partnerships.
2 Copies of the evidence of identity and address must be attached.
3 This form and supporting documents must be sent to the MLRO for filing.

APPENDIX C

DISCLOSURE FORMS

DISCLOSURE FORM – PART 1

Report to Money Laundering Reporting Officer

Details of Employee:

From _____ **Email/telephone** **Number** _____

1	**Are you dealing with a transaction which might be a prohibited act under sections 327-329 if the Proceeds of Crime Act 2002 and which requires appropriate consent from the NCA?**	**YES/NO**
2	**Details of Customer** **Identities of the person(s) subject to the enquiry** **Name** **(If a company/public body please indicate nature of business)** **Address** **Telephone Number (including area code)**	

3	**Copy of Identity Verification Form and evidence of identity attached?** **(If no, give reasons)**	**YES/NO**
4	**Summary of transaction and customer's role**	
5	**Value of transaction**	
6	**Amount and source of funds** **(e.g. cash, bank or other securities including account numbers)**	

7	**Destination of funds (including account numbers)**	
8	**Reason for suspicion**	
9	**Nature of suspicions**	
10	**To your knowledge, has any investigation been undertaken?**	**YES/NO**

	(If yes, please include details)	
11	**Have you discussed your suspicions with anyone else?** **(If yes please specify below with whom, explaining reasons for such discussion and the outcome of the discussion.)**	**YES/NO**
12	**Have you consulted any supervisory body for guidance?** **(e.g. NCA or professional body such as ICAEW). If yes please provide details**	**YES/NO**
13	**Do you feel you have a reasonable excuse for not disclosing the matter to NCA?** **If yes please give full details**	**YES/NO**

Signed _____ **Dated** _____

Once completed please forward this form to the MLRO. Please do not discuss the content of this report with anyone you believe to be involved in the suspected money laundering activity described. To do so may constitute a tipping off offence which carries a maximum penalty of 5 years imprisonment.

MONEY LAUNDERING DISCLOSURE FORM – PART 2

The following part of this form is for completion by the MLRO

DETAILS OF THE MLRO

Name _____

(insert name of MLRO/deputy MLRO)

Email /Telephone Number _____

Date report received _____

Date report acknowledged _____

1	**Report to NCA?** **If no please state reasons**	YES/NO

	If yes please confirm date of report to NCA.	
2	**Details of liaison with NCA regarding the report** **Name of NCA person spoken to** **Notice period** **Moratorium period**	 _____ to _____ _____ to _____
3	**Is consent required from the NCA to any ongoing or imminent transactions which would otherwise be prohibited acts?** **If yes has consent been obtained?** **Name of NCA person spoken to** **Contact details** **Date consent received from NCA** **Date consent given by you to employee**	YES/NO
4	**Report NCA?** **If no please state reasons**	YES/NO

5	**Date consent given by you to employee for any prohibited transactions to proceed**	
6	**Date business relationship /transaction completed**	
7	**Record destruction date (5 years from date at 6)**	

Signed _____ Dated _____

THIS REPORT TO BE RETAINED FOR AT LEAST FIVE YEARS UNLESS A REPORT HAS