Anti-money laundering policy

Anti-Money Laundering Policy

Policy Owner: Coporate Director Resources

23/11/2023

Table of Contents

Introduction

The Council is at risk of being used as a pathway to legitimise funds as a means of disguising their origins thus we may unknowingly be used as a means of ‘cleaning’ criminal funds. This carries both a corporate and personal responsibility so any person receiving funds on behalf of the Council must be aware of the policy and the path of reporting. The legal and strategic responsibility lies with the Council’s Section 151 Officer (Corporate Director of Resources) whilst any investigation and day to day compliance rests with the Investigations Manager (Anti-Fraud, Internal Audit, Risk and Insurance) who should be the first point of contact.

Policy statement

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**.**

The Scope of the policy

The This Policy applies to all officers and employees of London Borough of Tower Hamlets (the Council). 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.

All persons must be familiar with their legal responsibilities. Failure to comply may be a criminal offence and disciplinary matter.

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.

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.

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

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.

The Money Laundering Reporting Officer (MLRO) is the Corporate Director of Resources (Section 151 Officer) and they are responsible for the strategic management and adherence to the policy, whilst day to day oversight and investigation rests with the Investigations Manager (Anti-Fraud, Internal Audit, Risk and Insurance). However, all 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.

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

This Policy and guidance have been 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 because 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.

Introduction – What is money laundering?

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.

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.

If you are involved, in any way, in dealing with or facilitating an arrangement regarding '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.

Terrorists also need to launder money to fund their criminal enterprises. The acts of terrorism that have occurred over the years in the UK have focused attention on the need to enforce anti-money laundering rules to combat terrorists, as well as drug dealers and organised crime.

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.

The laundering process

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.

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

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.

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.

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.

How the Council could become involved in money laundering

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.

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

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.

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").

Risk assessments should also be conducted regularly to consider the 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.

Accountants, registered 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.

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, being asked to work with unusual types of client or on unusual types of matter, resistance from a client regarding compliance with due diligence checks, being pressured to forego necessary due diligence checks or to “speed up” the process, 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) and transactions where the business rationale 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 requirements.

Consequences

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.

Therefore, it is important that all persons understand this policy and always apply it.

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.

If there is anything you do not understand, please ask your manager, or direct queries to the MLRO or Investigations Manager, Rob Watt

The relevant law

The Proceeds of Crime Act 2002 (POCA)

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

- concealing, disguising, converting, or transferring criminal property or removing criminal property from the UK (section 327)
- entering or becoming concerned in an arrangement which a person knows, or suspects facilitates the acquisition, retention, use or control of criminal property (section 328)
- 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).

- 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).

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

If you are found guilty of any of the offences in paragraphs Proceeds of Crime Act 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.

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 (making a disclosure).

[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

The Terrorism Act 2000

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 any business relationship.

The list can be viewed at http://www.hm-treasury.gov.uk/fin_sanctions_index.htm

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.

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

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.

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

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.

Relevant Guidance – Assessing Risk

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.

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.

Having reviewed its risk profile, the senior management of the Council have approved a policy which embodies appropriate controls to manage and mitigate those risks. A minimum standard of identification is required for all. 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 (Customer Due Diligence Procedures) for more details. If in doubt regarding the level of risk in individual situations, you must seek advice from the MLRO.

Customer due diligence procedures

The Legal Requirement

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.

[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

Customer due diligence is more than just a box ticking exercise; it is each person's responsibility to risk assess each transaction.

The procedures must be applied 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, registered audit, or legal services, and where the Council expects, 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.

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

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

- 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
- The bodies or organisations designated as "public bodies" for the purposes of the Local Authorities (Goods and Services) Act 1970
- Partnership undertakings including the third sector.

The identity evidence must:

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

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

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.

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.

The Identification and Verification Process

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

Individual

full name

current residential address

previous address if the customer has changed address in the last three months

date of birth

nationality

country of residence

whether they constitute a Politically Exposed Person

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

full name of business

registered number

registered office

business address

country of incorporation

(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.

Trusts

full name of the Trust

nature of trust (discretionary, bare, etc)

donor of the funds

nature of business or activity

location of business or activity

country of establishment

names of all trustees

name of any protector or controller

names or classes of beneficiaries

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

registered name

registration number

address of the Charity Commission's correspondent for the charity.

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).

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).

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.

Partnerships (including LLPs) and unincorporated businesses, if very well known, (e.g., law and accountancy firms) may be treated as publicly quoted companies). 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.

Charities can take several 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 their website www.gov.uk/government/organisations/charity-commission

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.

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).

In most cases simplified due diligence will be sufficient. 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 (Enhanced due diligence for further information)

Banks and building societies are generally exempt from the verification requirements (see High Risk Transactions below), and much less stringent requirements apply where the company is listed or is FCA regulated.

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 records. 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.

As well as obtaining satisfactory evidence of the identity and address, all persons must complete an appropriate Identity Verification Form.

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.

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).

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

- 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
- update information held on the customer to ensure the information held is valid

- review information held on the customer to ensure it is current and valid; and
- monitor the customer's business activity and business transactions to ensure that the Council is not being used as a vehicle for money laundering.

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.

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, requiring transactions to be carried out through an account in the person's name with a UK or an EU regulated credit institution, making telephone contact on a verified home or business land line; and communicating at an address which has been verified.

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):

where the transaction is complex.

where the transaction is unusually large or

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).

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.

Politically Exposed Persons (PEPS)

If the customer is a PEP it is necessary to:

- obtain approval from the MLRO to proceed with establishing a business relationship with such a customer;
- establish the source of wealth and source of funds which are involved in the business relationship or occasional transaction; and
- conduct enhanced ongoing monitoring of the business relationship.

High risk transactions/customers

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 to ascertain whether the transaction is suspicious and whether disclosure is to be made. In addition, the source of the funds to be transferred should be ascertained.

Ongoing monitoring

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

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 customer.

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

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.

Financial institutions regulated by the FCA, 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.fca.org.uk).

Where a one-off transaction is carried out (but not where there is a business relationship) pursuant to an introduction effected by an FCA-regulated firm or individual, and that firm or individual has provided written assurance that satisfactory

[5] Regulation 27(2), 2017 Regulations

evidence of individual identity of the contact introduced by him has been obtained and recorded, evidence of identity is not required.

Where the customer is:

a publicly quoted company

a majority-owned and consolidated subsidiary of a publicly quoted company

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

nothing is required beyond the standard identification.

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 must undertake the checks and make a disclosure to the MLRO.

Information management issues

Data Protection

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 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

[6] Article 15, GDPR

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

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.

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]

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]

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.

The Council's Data Protection Policy can be viewed on the Council's intranet, Data Protection Policy (towerhamlets.gov.uk) 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 Information Governance Team at DPO@towerhamlets.gov.uk

[7] Schedule 2, part 1 of the Data Protection Act 2018
[8] Schedule 1, part 2 of the Data Protection Act 2018

Freedom of Information

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 the following exemptions.

- Information held by a public authority is exempt information
- if it was directly or indirectly supplied to a public authority by, or relates to various government bodies, which includes NCA (section 23)
- if its disclosure would, or would be likely to, prejudice the prevention or detection of crime or apprehension or prosecution of offenders (section 31).

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

Details on Freedom of Information can be viewed on the Council's Intranet at: Freedom of information (towerhamlets.gov.uk)

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

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

Making a disclosure

How to make an authorised disclosure – internal reporting procedures

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). 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.

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 A for pro-forma of this form. In no circumstances should a copy of the Disclosure Form be put on the file or otherwise disclosed to anyone other than the MLRO.

The Council requires all disclosures be made to the MLRO, Corporate Director, Resources.

If the MLRO is not available at the time you want to make a disclosure, the disclosure should be made to Rob Watt, Investigation Manager, telephone 07908 130194.

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.

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.

The offence of failing to disclose

If you know or suspect or, 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).

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 03 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.

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.

If the MLRO receives a disclosure report based on 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.

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

The Role of the MLRO

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.

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.

- reviewing other transaction patterns and volumes
- the length of any business relationship involved
- the number of any one-off transactions and linked one-off transactions; and
- any identification evidence held.

The MLRO must undertake such other reasonable inquiries he thinks appropriate to ensure that all available information is considered in deciding whether a report to

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

NCA is required (such enquiries being made in such a way as to avoid any appearance of tipping off those involved).

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.

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

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

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

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.

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

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.

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.

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 Tipping off below).

Legal professional privilege

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.

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.

Legal Advice Privilege

Legal advice privilege applies to.

- confidential communications which pass between members of the Council or other council staff and solicitors and other legal services' staff; and
- which have come into existence for the purpose of obtaining legal advice in relation to the business of the Council.

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.

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.

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.

Litigation privilege

Ligation privilege applies to:

- confidential communications when litigation is pending or contemplated which pass between members of the Council or other Council staff and solicitors and other legal services' staff; and
- 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.

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

Checks for Lawyers

Consider any unusual transactions and do appropriate due diligence particularly in relation to source of funds.

Carry out enhanced verification checks in relation to identity, property, trusts, monetary activity as a minimum.

Seek to understand the rationale for any litigation/business transactions.

Document any transactions and adopt a risk-based approach.

Monitor ongoing business/client relationships.

Ensure transactions are appropriate for the instructions.

Review existing records and consider the reasoning for every transaction/contract.

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

After a disclosure has been made

Caution

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, if the MLRO decides to make an SAR.

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 (under Tipping off).

Consent

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

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.

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.

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.

Tipping off

At no time and under any 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.

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.

What Is suspicious?

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 circumstances, be likely to trigger suspicion:

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.

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

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

Any request to hold sealed boxes/parcels.

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

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.

Overpayments by any party.

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.

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

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.

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.

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

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

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

Poor business records and internal accounting controls.

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

A transaction which is unusually large, or small.

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

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 (refer to www.fatf-gafi.org).

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.

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.

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

Anything which seems too good to be true.

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.

Record keeping procedures

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:

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

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 during the one-off transaction or the last one-off transaction where linked; and

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

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.

Training

The Regulations require that 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]

The MLRO will ensure that all relevant staff undergo an electronic training course on money laundering which covers the legislation, an explanation of what money laundering is, what is likely to amount to suspicious activity and the processes and procedures to be followed to comply with this policy. All persons will be required to undertake updated training as necessary (to be determined by the MLRO).

The MLRO will maintain records of appropriate training given to each officer and employee.

[12] Regulation 24 of the 2017 Regulations.

If any person is contacted by NCA, the police, HM Revenue and Customs or any other law enforcement body regarding 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.

Summary of responsibilities

All relevant persons must:

1. Read and follow this policy.
2. Know and understand the legislation.
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.
4. Always remain vigilant and alert to suspicions.
5. Report any suspicions to the Money Laundering Reporting Officer (MLRO) in accordance with internal procedures.
6. Complete the multimedia training programme and pass the test to reinforce understanding of the law, internal rules, and procedures.
7. Keep appropriate records for at least five years, and indefinitely in cases where an SAR has been made.

The MLRO must.

Monitor compliance.

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

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

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

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

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

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

Appendix A

Anti-Money Laundering Reporting Form

Your contact details
Please provide your contacts details in the box below so we can confirm that we have received the report and get into contact with you if required.

Name:	
Role:	
Email:	
Contact Telephone:	

Main subject

Please provide the details of the person you suspect of money laundering. If you suspect more than one person, please fill in the additional boxes below.

Name:	
Date of Birth:	
Gender:	
Occupation:	
Address	Type: (Home, work etc)

Transaction(s)
Please enter the details of the transactions you think are suspicious

Date:	
Amount:	
Currency:	
Credit/Debit	
Reason for the transaction:	

Date:	

Amount:	
Currency:	
Credit/Debit	
Reason for the transaction	

Account(s)
Please enter details of the account(s) used.

Account Holder's Name	
Acc. No	
Sort Code:	
Current balance:	
Balance date:	

Account Holder's Name	
Acc. No	
Sort Code	
Current balance:	
Balance date:	

Associated subjects
If there are any other people you suspect are involved in money laundering, please enter their details.

Name:	
Date of Birth:	
Gender:	
Occupation:	
Reason for association	
Address	
Type: (Home, work etc)	

Name:	
Date of Birth:	
Gender:	
Occupation:	
Reason for association	
Address	
Type: (Home, work etc)	

Linked addresses
Please enter details of any linked addresses:

Address Type: (Home, work etc)

Reason for suspicion

Please enter details of your suspicions. Please provide as much information as possible.