London Borough of Merton

ANTI-MONEY LAUNDERING POLICY

Date of Review: April 2023

Date for next review: April 2026

1. Introduction

1.1. On 10 January 2020 changes to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (SI No. 2017/692) (the MLRs) came into force. The changes update the UK's Anti Money Laundering regime to incorporate international standards set by the Financial Action Task Force (FATF). The Money Laundering and Terrorist Financing (Amendment) Regulations 2019 (the 2019 Regulations) amend the MLRs. Further amendments to the MLRs by the Money Laundering and Terrorist Financing (Amendment) (No.2) Regulations 2022 (No. 860) made on 21 July 2022 came into force in stages in accordance with regulation 1.

1.2. As an overview, the changes incorporate the requirement to keep an up to date list of exact functions that qualify as prominent public functions, the requirement on enhanced due diligence when working with high risk countries, the requirement to maintain registers of beneficial owners, a reduced limit of pre-paid cards and electronic money, enhanced due diligence on virtual currencies/crypto currencies/digital tokens and letting agency activities to be brought within the scope of Anti-Money Laundering.

1.3. A key difference is the Fifth Money Laundering Directive brings additional businesses into the scope of the anti-money laundering regulatory framework. Described as “obliged entities” in the Fourth Money Laundering Directive, these are defined as “relevant persons” in the MLRs and as businesses in the “regulated sector” in the Terrorism Act 2000 (the 2000 Act) and the Proceeds of Crime Act 2002 (the 2002 Act). The requirements of the Fifth Money Laundering Directive do not allow for the exemption of small businesses, or any exemptions based on size.

1.4. In identifying ownership, the 2019 Regulations introduce an explicit Customer Due Diligence (CDD) requirement for relevant persons to take reasonable measures to understand the ownership and control structure of their customers. Relevant persons must also take reasonable measures to verify the identity of senior managing officials when the beneficial owner of a body corporate cannot be identified.

1.5. Although Anti-Money Laundering legislation does not specifically cover local authorities as defined by organisations in the regulatory sector, it is implied best practice that we assess the risk and put sufficient controls in place to prevent the Council from being used for money laundering.

2 Scope

2.1 This Policy applies to all of the Council’s activities, its employees, including those permanently employed, temporary staff, agency staff, contractors, Members (including independent members), volunteers and consultants.

2.2 It is important that all employees are familiar with their responsibilities as serious criminal sanctions may be imposed for breaches of anti-money laundering legislation. Failure by any member of staff to comply with this Policy may lead to prosecution and disciplinary action being taken against them. Any disciplinary action will be dealt with in accordance with the Council's Disciplinary Procedures.

2.3 Whilst it is stressed that the risk to the Council is low, it is extremely important that all staff are familiar with their legal responsibilities as serious criminal sanctions may be imposed for breaches of the legislation. The key requirement for staff is to:

- ***Promptly report any suspected money laundering activity to the Money Laundering***

Reporting Officer (MLRO).

3 What are the obligations on the Council?

3.1 As noted at paragraph 1.5 above, whilst local authorities are not directly covered by the requirements of the MLRs, guidance from finance and legal professions, including the Chartered Institute of Public Finance and Accounting (CIPFA), indicates that public service organisations should comply with the underlying spirit of the legislation and regulations and put in place appropriate and proportionate anti-money laundering safeguards and reporting arrangements.

3.2 The MLRs, as amended, by the 2019 Regulations apply to "relevant persons" acting in the course of business carried out by them in the UK. Relevant persons must check beneficial ownership registers of legal entities in scope of the People with Significant Control (PSC) requirements before establishing a business relationship. Where there is a discrepancy between the beneficial ownership information on the registers and the information that is made available to them in the course of carrying out CDD, there is a requirement to report these discrepancies to Companies House. Companies House will investigate and, if necessary, resolve the discrepancy in a timely manner. These reports are excluded from public inspection. For the purposes of the MLRs, not all of the Council's business is relevant, it could include accountancy and audit services carried out by Financial Services and the financial, company and property transactions undertaken by the Council's Shared Legal Service, the South London Legal Partnership.

3.3 The obligations on the Council are to establish and maintain appropriate and risk-sensitive policies and procedures relating to the following:

- customer due diligence measures and ongoing monitoring.
- reporting.
- record-keeping.
- internal control.
- risk assessment and management; and
- the monitoring and management of compliance with, and the internal communication of such policies and procedures.

3.4 All employees are required to follow the procedure set out in this Policy and in this way the Council will properly discharge its obligations under the money laundering regime.

4. Background

4.1. Money laundering is the term used for a number of offences involving the proceeds of crime or terrorist financing: Such offences are defined under the 2002 Act as the following prohibited acts:

- concealing, disguising, converting, transferring, or removing criminal property from the United Kingdom
- becoming concerned in an arrangement which facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person, either knowingly or merely by way of suspicion.
- acquiring, using, or possessing criminal property
- doing something that might prejudice an investigation e.g., falsifying a document
- failure to disclose one of the offences listed above where there are reasonable grounds for knowledge or suspicion; and/or
- tipping off a person(s) who is suspected of being involved in money laundering in such a way as to reduce the likelihood of or prejudice an investigation.

4.2. Although the term ‘money laundering’ is generally used when describing the activities of organised crime, for which the legislation and regulations were first and foremost introduced, to most people who are likely to come across it, or be affected by it, it involves a suspicion that someone they know, or know of, is benefiting financially from dishonest activities.

4.3. Money laundering activity may range from a single act, for example being in possession of the proceeds of one’s own crime, to complex and sophisticated schemes involving multiple parties and multiple methods of handling and transferring criminal property as well as concealing it and entering into arrangements to assist others to do so. Council employees need to be alert to the risks of clients, their counterparties and others laundering money in any of its many forms.

4.4. Under Section 18 of the 2000 Act, it is an offence for a person to enter into or become concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property: -

(a) by concealment,

(b) by removal from the jurisdiction,

(c) by transfer to nominees, or

(d) in any other way.

“Terrorist property” is defined by Section 14 of the 2000 Act as money or other property which is likely to be used for the purposes of terrorism (including any resources of a proscribed organisation), proceeds of the commission of acts of terrorism, and proceeds of acts carried out for the purposes of terrorism.

4.5 In recent years, new laws have been passed which significantly shifts the burden of identifying acts of money laundering away from government agencies and more towards organisations and their employees. They prescribe potentially very heavy penalties, including imprisonment, for those who are convicted of breaking the law.

4.6 It is vital to recognise that the regime under which money laundering is monitored operates on an ‘all crimes’ basis, and that there is no *de minimis* provision in the money laundering legislation. In other words, every crime, however small, is subject to the money-laundering regime.

5 High Risk Areas

5.1 In order to minimise the risk of money laundering when dealing in high-risk areas, or where customers or clients meet any of the criteria below, an Identification Procedure must be followed before any business is undertaken with that organisation or person

- Undertake a one-off transaction involving payment by or to the client of 15,000 Euro (approximately £13,500) or more.
- Undertake a series of linked one-off transactions involving total payment by or to the client of 15,000 Euro (approximately £13,500) or more.
- It is known or suspected that a one-off transaction (or a series of them) involves money laundering.

5.2 The Council is committed to raising awareness and where necessary specific guidance and training will be provided to services assessed at high risk of money laundering and terrorist financing.

6 Identification Procedures and Customer Due Diligence

6.1 For any new business relationship or any business involving a considerable one-off transaction the officer concerned should set up and maintain identification procedures regarding the parties involved, in particular, if the new party is not present or acting on behalf of a third party. Satisfactory evidence must be obtained as soon as practicable after instructions are received and should be capable of establishing, to the satisfaction of the person receiving it, that the client is who they claim to be. Documentary evidence i.e., birth certificate, drivers' licence, a power of attorney, signed written instructions on headed paper is an example of what can be obtained for this procedure.

6.2. Where the Council is carrying out certain regulated business (accountancy, audit and tax services and legal services in relation to financial, company or property transactions) Identification Procedures and Customer Due Diligence checks should be undertaken.

6.3 These checks should be done as soon as practicable after instructions are received (unless evidence has already been obtained) and no dealings should take place until this has been completed.

6.4 Satisfactory evidence is evidence which establishes that the client (company and/or person) is who they claim to be. This can include, but is not limited to, some of the following:

- Signed, written instructions on official letterhead at the outset of the dealings, which confirms the company name and location
- Verification of company registration and VAT numbers, website details and registered office address
- checking with the customer/supplier's website to confirm their business address.
- conducting an on-line search via Companies House to confirm the nature and business of the customer and confirm the identities of any directors.
- Proof of personal identification, if dealing with an individual, through meeting the client in person and verifying their identity against the passport or photo-card driving licence.
- Copies of the identity evidence obtained must be retained on file for at least five years. This retention can be in an electronic format (e.g., scanned documentation) as long as it is available for inspection with sufficient notice.

7. Customer Due Diligence

7.1 Customer due diligence means that the Council must know its clients and understand their businesses. This is to enable the Council to be in a position to know if there is suspicious activity that should be reported. Clearly, it is only by the Council knowing its clients and their businesses that it can recognise abnormal and possibly suspicious activity.

7.2 The obligations imposed on the Council must, of course, be brought into effect by its individual employees. Employees must therefore be familiar with these obligations.

7.3 The MLR, as amended by the 2019 Regulations, require that the Council identifies its customers and verifies that identity based on documents, data or information obtained from a reliable source. Where there is a beneficial owner who is not the customer then the Council must identify that person and verify the identity and where the beneficial owner is a trust or similar then the Council must understand the nature of the control structure of that trust.

7.4 The Council must obtain information on the purpose and intended nature of the business relationship. Under Regulation 33(1)(b) of the MLRs, Enhanced Customer Due Diligence (ECDD) is required for any business relationship with a person established in a high-risk third country.

7.5 From 1 January 2021, the UK has had its own standalone list of high-risk third countries. (Any amendments to the EU List do not have effect in the UK). The UK can amend its own list of high-risk countries under Section 49 of and Schedule 2 to, the Sanctions and Anti Money Laundering Act 2018 and has announced proposals to align further with Financial Action Task Force (FATF) practices. The list of high-risk third countries in Schedule 3ZA to the MLRs was substituted with effect from 12 July 2022 by Regulation 2 of the Money Laundering and Terrorist Financing (High-Risk Countries) (Amendment) (No 2) Regulations 2022 (SI 2022/782).

7.6 The checks described in paragraph 7 must generally be undertaken by the Council: -

- before it establishes a business relationship; or
- carries out an occasional transaction; or
- if it suspects money laundering or terrorist financing; or
- doubts the veracity of any information obtained for the purposes of identification or verification.

However, the Council is not required to undertake these checks if its customer is another public authority, unless it suspects money laundering or terrorist financing.

7.7 The Council is also obliged to undertake ongoing monitoring of its business relationships which means it must scrutinise transactions throughout the course of the relationship to ensure that the transactions are consistent with the Council's knowledge of the customer and keep the information about the customer up to date.

7.8 Where property transactions are carried out using externally appointed agents on behalf of the Council, the agent will be required to perform and evidence Customer Due Diligence checks, and these should be shared and retained by the Council.

7.9 Where the Council is not able to apply the Customer Due Diligence measures set out above: -

- it must not carry out a transaction with or for a customer through a bank account.
- it must not establish a business relationship or carry out an occasional transaction with the customer.
- it must terminate any business relationship with the customer and consider whether to make a disclosure.

7.10 However, paragraph 7.9 does not apply where a lawyer or other professional adviser is in the course of advising on the legal position for his/her client or performing his/her task of defending or representing that client in, or concerning, legal proceedings including the advice on the institution or avoidance of proceedings.

8. Enhanced Customer Due Diligence and Ongoing Monitoring

8.1 It will in certain circumstances be necessary to undertake Enhanced Customer Due Diligence as set out in paragraphs 7.4 – 7.5 above. In summary, this will be necessary where:

- the customer has not been physically present for identification purposes; or
- in any other situation which by its nature can present a higher risk of money laundering or terrorist financing.

8.2 Where this applies, the Council will need to take adequate measures to compensate for the higher risk. For example, this will mean ensuring that the customer's identity is established by additional documents, data or information.

8.3 Similarly, where the Council is in an ongoing "business relationship" with a customer, the MLRs impose a special obligation to carry out ongoing monitoring. This means that the Council must:

- scrutinise transactions undertaken throughout the course of the relationship to make sure that these transactions are consistent with the Council's knowledge of the customer, his/her business, and risk profile; and
- keep documents, data or information obtained for the purpose of applying Customer Due Diligence measures up to date.

8.4 The MLRs require that Enhanced Customer Due Diligence measures are taken to manage and mitigate the risks posed by a politically exposed person (PEP). The term PEP means an individual who is entrusted with prominent public functions, other than as a middle-ranking or more junior official. The Council is required to have appropriate risk-management systems and procedures to identify when the customer is a PEP and to manage the enhanced risks arising from having a relationship with that customer. Business relationships with a *family member* or a *known close associate* of a PEP are also subject to greater scrutiny.

9 When Money Laundering is suspected

9.1 Where you know or suspect that money laundering or terrorist financing activity is taking/has taken place, or you are concerned that your involvement in the matter may amount to a prohibited act under the anti-money laundering legislation, you must disclose this suspicion or concern to the Council's Money Laundering Reporting Officer (MLRO) as soon as practicable. The disclosure should be made within hours rather than days or weeks of the information coming to your attention. The MLRs stipulate that a single cash transaction, or a series of linked transactions, totalling over €15,000 (approximately £13,500 at the time of the legislation) should be treated as suspicious. However, vigilance also needs to be maintained in respect of all other possibilities such as a series of smaller payments in cash.

9.2 Any necessary investigation will be undertaken by the National Crime Agency (NCA) or relevant successor body, as appropriate. All members of staff will be required to co-operate with the MLRO and the authorities during any subsequent money laundering investigation.

9.3 Similarly, **at no time and under no circumstances should you raise any suspicions** with the person(s)/organisation you suspect of money laundering or terrorist financing, otherwise you may commit the criminal offence of "tipping off".

9.4 Accordingly, no reference should be made on a client file to a report having been made to the MLRO. Should the client exercise his/her right to see the file then such a reference would obviously tip them off to the report having been made. Again, you would be at risk of prosecution for the offence of "tipping off". The MLRO will keep the appropriate records in a confidential manner.

9.5 After reporting the employee:

- must follow any subsequent directions of the MLRO and must not themselves make any further enquiries into the matter.
- must not take any further steps in any related transaction without authorisation from the MLRO.
- must not disclose, or otherwise indicate, their suspicions to the person suspected of the money laundering.
- must not discuss the matter with others as this can result in "tipping off" the suspect
- must not record on the file that a report has been made to the MLRO in case this results in the suspect becoming aware of the situation and could constitute a "tip

off".

9.6 Employees should be aware that:

- Ignoring the obvious can be considered a criminal offence.
- A reasonable cause for knowledge or suspicion of money laundering offence will be required. Speculation or gossip is unlikely to be sufficient to justify an investigation.
- The size or significance of the money laundering offence is irrelevant as money laundering covers the proceeds of any crime, no matter how minor and irrespective of the size of the benefit gained.

10 Money Laundering Reporting Officer (MLRO)

10.1 The Council has nominated ***Margaret Culleton***, the Head of Internal Audit, to be its MLRO, to whom disclosures about money laundering activity should be made. Contact details are as follows:

Head of Internal Audit,
London Borough of Merton
Civic Centre
London Road
Morden
SM4 5DX

Email: Margaret.culleton@merton.gov.uk

10.2 The MLRO is responsible for ensuring that sufficient guidance is available to officers identified as working in areas of higher risk of money laundering or terrorist financing; and for maintaining a central register of reportable incidents which are promptly assessed and, where disclosure is deemed necessary, reported to the NCA.

10.3 Upon receipt of the disclosure report, the MLRO will:

- Consider it and any other available internal information the MLRO considers relevant.
- Undertake such further reasonable inquiries the MLRO considers appropriate.
- Seek specialist legal and financial advice, if necessary.
- Promptly evaluate any disclosure, and determine whether it should be reported to the NCA: - by way of a Suspicious Activity Report (SAR) (form can be located on the NCA website)

10.4 The MLRO will commit a criminal offence if s/he knows or suspects, or has reasonable grounds to do so, through a disclosure being made, that another person is engaged in money laundering, but does not disclose it to the NCA as soon as practicable.