BARNSLEY
Metropolitan Borough Council

Corporate Anti-Money Laundering Policy (and Guidance)

Table of Contents

1. INTRODUCTION

1.1 The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (referred to throughout this policy as MLR 2017) came into force on 26 June 2017. They implement the EU's 4th Directive on Money Laundering. In doing so, they replace the Money Laundering Regulations 2007 and the Transfer of Funds (Information on the Payer) Regulations 2007 which were previously in force.

1.2 Barnsley Council is committed to establishing and maintaining effective arrangements to prevent and detect attempts to launder money using Council services. The Council requires all Members and employees to demonstrate the highest standards of honesty and integrity and this includes compliance with appropriate legislation. The Council is committed to working constructively with the Police and other relevant agencies in relation to combating money laundering and ensuring compliance with the legislation.

1.3 This policy is designed to set out the Council's approach to money laundering prevention and associated reporting and should be read in conjunction with the Council's Anti-Fraud and Corruption Policy. The Council will seek to ensure the corporate stance on money laundering is widely publicised and that employees and Members have access to the appropriate guidance. Failure to comply with the procedures set out in this document may constitute a disciplinary and/or criminal offence.

2. SCOPE

2.1 This policy applies to all employees of the Council, including temporary and agency staff as well as those employed in locally maintained schools. It contains specific sections to advise employees of the process to be followed to enable the Council to comply with its legal obligations. This policy is also applicable to elected members where any suspicions of money laundering activity are noted or come to light

2.2 The aim of the policy is to ensure all appropriate action is taken to prevent, wherever possible, the Council, its Members and employees from being exposed to money laundering and to comply with all legal and regulatory obligations.

3. WHAT IS MONEY LAUNDERING?

3.1 Money Laundering is the process by which criminally obtained money or other criminal property is exchanged for "clean" money or other assets with no obvious link to their criminal origins. The term is used for a number of offences involving the integration of "dirty money" (i.e. the proceeds of crime) into the mainstream economy. The aim is to legitimise the possession of such monies through circulation and this effectively leads to "clean" funds being received in exchange. It is a favoured method of organised criminals and terrorists.

3.2 The term "Money Laundering" describes offences involving the integration of the proceeds of crime, or terrorist funds, into the mainstream economy. Such offences are defined under The Proceeds of Crime Act 2002 and the primary ones are listed below;

- Concealing, disguising, converting or transferring criminal property or removing it from the UK;

- Entering into or becoming concerned in an arrangement which you know or suspect facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person;
- Acquiring, using or possessing criminal property;
- Failure to disclose knowledge or suspicion of another person(s) involvement in money laundering; and
- Tipping off (a person) or making a disclosure which is likely to prejudice an investigation being carried out by a law enforcing authority, knowing that such an investigation is in motion.

Further details are provided in **Appendix A: Offences Table**:

3.3 Offences cover a range of activities (not necessarily involving money or laundering) regarding the proceeds of crime. This means that potentially any employee or Member, irrespective of what sort of Council business they are undertaking, could commit an offence if they become aware of, or suspect the existence of criminal property, irrespective of the size of the benefit gained, and/or fail to report their concerns.

3.4 Where an employee/Member suspect money laundering and report, or are aware that someone else has, they must exercise caution in what is discussed with others as a further offence of "tipping off" may be committed if, knowing or suspecting a disclosure has been made, the employee/Member take any action which is likely to prejudice any investigation that may be conducted.

3.5 It is impossible to give a definitive list of ways in which to spot money laundering or how to decide whether to make a report. Money laundering activity may range from a single act such as the use of criminal funds to pay an invoice to multiple payments to an account to "launder" money in smaller chunks to avoid checks and suspicions. They can even involve 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.

3.6 Council employees need to be alert to the risks of money laundering in any of its many forms. Facts which tend to suggest that something 'odd' is happening may be sufficient for a reasonable suspicion of money laundering to arise. Risk factors which may, either alone or cumulatively with other factors suggest the possibility of money laundering activity are provided at **Appendix B: Possible Signs of Money Laundering**.

3.7 Potentially any employee or Member could be caught by the money laundering provisions if they suspect money laundering and either become involved with it in some way and/or do nothing about it. They may be liable to prosecution and, if convicted of one of the offences listed above, may receive an unlimited fine and up to 14 years imprisonment. (Section 7 of this document provides guidance regarding the reporting of, and implications of the failure to report, suspicions of money laundering).

4. REQUIREMENTS OF THE MONEY LAUNDERING LEGISLATION

4.1 The MLR 2017 imposes specific obligations on "relevant persons".

4.2 The term relevant person relates to the following activities carried out in the course of business; tax advice; accounting services; treasury management; investment or other financial services; credit institutions; audit services; legal services; estate agents; services involving the formation, operation or arrangement of a company or trust; dealing in goods wherever a transaction involves a cash payment equivalent to €15,000 or more.

4.3 The obligations include the following requirements:

- Appoint a Money Laundering Reporting Officer (**MLRO**).
- Obtain sufficient knowledge to ascertain the true identity of customers in certain circumstances, by applying **customer due diligence** measures.
- Know the intended nature of business relationships and undertake ongoing monitoring of them (to identify **unusual transactions**).
- Implement a procedure for assessing and controlling risk and **reporting suspicions** of money laundering.
- Maintain **record keeping** procedures (e.g. for evidence of identity obtained, details of transactions undertaken, for at least 5 years afterwards).

4.4 Local Authorities are not directly covered by the requirements of the MLR 2017. However, some activities undertaken by local authorities could be included within the scope of the regulations and 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.

4.5 To ensure compliance with the regulations and legislation, the Council are considered a relevant person when acting in the course of business and activities carried out by them.

4.6 The European Union's 4th Money Laundering Directive requires a focus on risk assessments in relation to anti-money laundering; in particular the need to evidence that an organisation's exposure to risk is considered as part of ongoing business. As such Heads of Service should maintain engagement with Internal Audit as business operations change with regard to undertaking appropriate and proportionate assessments.

5. THE MONEY LAUNDERING REPORTING OFFICER (MLRO)

5.1 If an individual becomes aware that their involvement in a matter may amount to money laundering then they must report it to the Money Laundering Reporting Officer (MLRO) and not take any further action until they have received consent from the MLRO, who may have to be granted such consent by the National Crime Agency.

5.2 The Council has designated the Head of Internal Audit, Anti-Fraud and Assurance as the MLRO:

Rob Winter Telephone Number: 01226 773241
Email: robwinter@barnsley.gov.uk

The Service Director Finance has been designated as Deputy MLRO:
Neil Copley Telephone Number: 01226 773237
Email: NeilCopley@Barnsley.gov.uk

5.3 The MLRO is responsible for:

- receiving internal suspicious activity reports (SARS) from within the Council;
- deciding whether these should be reported to the NCA;
- if appropriate making such reports to the NCA; and
- providing guidance and advice as necessary on money laundering matters/issues.

5.4 The MLRO will retain copies of the internal reports and copies of the decisions taken on each of the reports

6. CUSTOMER DUE DILIGENCE PROCEDURE

What is Due Diligence?

6.1 Regulations 27 and 28 of the MLR 2017 requires the Council to take steps to identify its customer and verify they are who they say they are. This is known as customer due diligence and, in practice, means obtaining a customer's:

- name
- photograph on an official document which confirms their identity
- residential address and date of birth

6.2 The best way to do this is to ask for a government issued document like a passport, along with utility bills, bank statements and other official documents. Other sources of customer information include the electoral register and information held by credit reference agencies such as Experian and Equifax.

6.3 In certain situations it may be necessary to identify the 'beneficial owner'. This may be because someone else is acting on behalf of another person in a particular transaction, or it may be because the ownership structure of a company, partnership or trust needs to be established.

6.4 As a general rule, the beneficial owner is the person who is behind the customer and who owns or controls the customer, or, it is the person on whose behalf a transaction or activity is carried out.

6.5 Officers must stop dealing with customers where there are doubts about identity.

Customer Due Diligence when Establishing a Business Relationship

6.6 A business relationship is one commenced where both parties expect that the relationship will be ongoing. It can be a formal or an informal arrangement.

6.7 The following information is required when establishing a new business relationship:

- the purpose of the relationship
- the intended nature of the relationship - for example where funds will come from, the purpose of transactions, and so on

6.8 The type of information needed may include:

- details of your customer's business or employment
- the source and origin of funds that your customer will be using in the relationship
- copies of recent and current financial statements
- details of the relationships between signatories and any underlying beneficial owners
- the expected level and type of activity that will take place in your relationship

6.9 A flowchart summarising the customer due diligence procedure is shown at **Appendix C** and a Verification of Customer Identity form is shown at **Appendix D.**

When is it Carried Out?

6.10 The requirement for customer due diligence applies immediately for new customers. However, it also allows organisations to vary customer due diligence according to the risk of money laundering or terrorist financing, depending on the type of customer, business relationship, product or transaction. This recognises that not all customers present the same risk, for example there is no need to apply customer due diligence measures where the customer is a UK public authority

6.11 Ongoing customer due diligence must be carried out during the life of a business relationship, proportionate to the risk of money laundering and terrorist funding, based on the officer's knowledge of the customer, regular scrutiny of the transactions involved and any changes of circumstances with the customer e.g. a big change in the level or type of business activity or a change in the ownership structure of a business.

6.12 Where there is a need to not interrupt the normal conduct of business and there is little risk of money laundering occurring and terrorist funding occurring, verification may be carried out during the establishment of the business relationship provided that the verification is completed as soon as practicable after the contact is first established

Enhanced Due Diligence (EDD)

6.13 Regulation 33(1) sets out a list of circumstances in which EDD measures must be applied (in addition to the customer due diligence measures detailed above).

6.14 These include any transaction or business relationship involving:

- any case identified as one where there is a high risk of money laundering or terrorist financing
- any business relationship or transaction with a person established in a high-risk third country;
- correspondent relationships with a credit institution or a financial institution (in accordance with regulation 34);

- a **Politically Exposed Person** (PEP) or a family member or known close associate of a PEP;
- in any case where the relevant person discovers that a customer has provided false or stolen identification documentation or information and the relevant person proposes to continue to deal with that customer;
- in any case where:
  - a transaction is complex and unusually large, or there is an unusual pattern of transactions, and
  - the transaction or transactions have no apparent economic or legal purpose, and
  - in any other case which by its nature can present a higher risk of money laundering or terrorist financing.

6.15 Under the regulations EDD measures must include, as a minimum, examining the background and purpose of the transaction and increasing monitoring of the business relationship.

6.16 Regulation 33(6) sets out a list of factors that must be taken into account in assessing whether there is a higher risk of money laundering and terrorist financing present in a given situation and the extent of EDD measures that should be applied. Whilst these factors should be taken into account, the situation should be considered as a whole i.e. the presence of one or more of the risk factors identified in 33(6) is not in itself determinative of a higher risk situation.

Politically exposed persons (PEPs)

6.17 The parts of MLR 2007 which applied only to foreign PEPs now also apply to local PEPs. This in practice means enhanced due diligence requirements for a broader range of individuals who have been trusted with prominent public functions both in the UK and overseas.

Simplified Customer Due Diligence

6.18 The circumstances in which simplified customer due diligence is permissible is more restricted under MLR 2017.

6.19 As part of the risk based approach, there ceases to be "automatic" simplified due diligence requirements for any transactions. Instead, a relevant person needs to consider both customer and geographical risk factors in deciding whether simplified due diligence is appropriate.

6.20 Simplified due diligence is permitted where you determine that the business relationship or transaction presents a low risk of money laundering or terrorist financing, taking into account your risk assessment.

Service Managers Responsibilities

6.21 The Council does not normally in the course of most of its duties undertake “regulated activities” for which additional checks and measures are necessary (*“due diligence”* checks). However, some Council activities are considered to be higher risk. On such transactions we

must ensure that we comply with the spirit of the money laundering regulations. These activities include (but are not limited to):

- Any advice given on tax affairs or accounting / auditing services done for other parties;
- Legal services;
- Property sales (commercial and those of housing stocks);

6.22 It is the responsibility of service managers to ensure that their systems of internal control are robust and that employees are appropriately trained in respect of money laundering. It is also the responsibility of service managers to ensure that appropriate due diligence checks are undertaken on any relevant transactions.

7. REPORTING PROCEDURE FOR SUSPICIONS OF MONEY LAUNDERING

7.1 Where an employee or Member suspects money laundering activity they must disclose this as soon as practicable to the MLRO. The disclosure should be within “hours” of the information coming to your attention, not weeks or months later.

7.2 Disclosures should be made to the MLRO using the standard pro-forma report attached at Appendix E. The report must include as much detail as possible, for example:

- Full details of the people involved (including employee or Member, if relevant);
- Full details of the nature of their involvement;
- The types of money laundering activity involved (see Appendix A, Offences Table);
- The dates of such activities, including whether the transactions have happened, are ongoing or are imminent;
- Where they took place;
- How they were undertaken;
- The (likely) amount of money/assets involved;
- Exactly why there are suspicions; the NCA will require full reasons;
- Any other relevant available information to enable the MLRO to make a sound judgment as to whether there are reasonable grounds for knowledge or suspicion of money laundering and to enable them to prepare their report to the NCA, where appropriate.

7.3 If an employee or Member becomes concerned that their own involvement in a transaction would amount to an offence under Sections 327 – 329 of the Proceeds of Crime Act 2002 or Regulations 86-88 of the MLR 2017 (see appendix A), then the report must include all relevant details. Consent will be required from the NCA, via the MLRO, for the individual to take any further part in the transaction. This is the case even if the customer gives instructions for the matter to proceed before such consent is given. Employees and Members should therefore make it clear in the report if such consent is required and clarify whether there are any deadlines for giving such consent e.g. a completion date or court deadline.

7.4 Once the matter has been reported to the MLRO then any subsequent directions provided must be followed. Further enquiries into the matter should not be made by the employee or Member; any necessary investigation will be undertaken by the NCA.

7.5 Reference of any reports being made to the MLRO should not be recorded on client files – should the client exercise their right to see their records, then such a note/reference will tip them off to the report having been made and may render the employee or Member liable to prosecution. The MLRO must keep the appropriate records in a confidential manner

7.6 Suspicions of money laundering, whether reported to the MLRO or not, must not be discussed with anyone else. Any discussions may account to an offence of 'tipping off'. Any person found guilty of tipping off or prejudicing an investigation offence is liable to imprisonment (maximum five years), a fine or both.

7.7 A new criminal offence was created in 2017: 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.

8. CONSIDERATION OF DISCLOSURE

8.1 The MLRO must note on the face of the disclosure report the date it was received, acknowledge receipt of the document and advise the employee or Member submitting the report of the timescale for a response.

8.2 The MLRO will consider the report and any other relevant internal information available, for example:

- 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.

8.3 The MLRO will undertake other reasonable enquiries considered appropriate in order to ensure that all available information is taken into account in deciding whether a report to the NCA is required The MLRO may also need to discuss the disclosure report with the employee or Member who submitted the report.

8.4 Once the MLRO has evaluated the disclosure report 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 they need to seek consent from the NCA for a particular transaction to proceed.

8.5 Where the MLRO suspects money laundering is taking place then they must disclose the matter as soon as practicable to the NCA on their standard report form and in the prescribed manner, unless they have a reasonable excuse for non-disclosure to the NCA (for example, you wish to claim legal professional privilege for not disclosing the information). Up to date forms can be downloaded from the NCA website at www.nationalcrimeagency.gov.uk

8.6 Where the MLRO considers no money laundering is taking place or suspects money laundering but has a reasonable excuse for non-disclosure, then he must note the report

accordingly and can then immediately give their consent for any ongoing or imminent transactions to proceed. However, it's better to disclose than not.

8.7 In cases where legal professional privilege may apply, the MLRO must liaise with the Service Director, Legal Services, to decide whether there is a reasonable excuse for not reporting the matter to the NCA.

8.8 Where consent is required from the NCA for a transaction(s) to proceed, then the transaction(s) in question must not be undertaken, completed or proceed until the NCA has specifically given consent, or there is deemed consent through the expiration of the relevant time limits without objection from the NCA.

8.9 Consent will be received in the following way:

- **Specific consent** (where the NCA have granted a defence against money laundering charges in their reply to the SAR);
- **No refusal of consent during the notice period** (seven working days starting with the first working day after the MLRO makes the disclosure). If a reply from the NCA is not received within 7 working days and the MLRO believes the activity has been correctly reported, s/he can choose to assume a defence is granted;
- Where the NCA reply to the SAR refusing permission to proceed, they have a further 31 calendar days to take action. If a **response has not been received after the 31 days**, the MLRO can proceed with the transaction. No offence will be committed.

8.10 The MLRO should therefore make it clear in the report if such consent is required, and clarify whether there are deadlines for giving such consent, e.g. completion date or court deadline.

8.11 Where the MLRO concludes that there are no reasonable grounds to suspect money laundering then the MLRO shall mark the report accordingly and give her consent for any ongoing or imminent transaction(s) to proceed.

8.12 All disclosure reports referred to the MLRO and reports made by them to the NCA must be retained by the MLRO in a confidential file kept for that purpose, for a minimum of five years.

8.13 The MLRO may commit a criminal offence under section 331 of the Act if he knows or suspects (or has reasonable grounds to do so) through a disclosure being made, that another person is engaged in money laundering and does not disclose this as soon as practicable to the NCA.

9. RECORD KEEPING AND RECORD RETENTION

9.1 Each department undertaking due diligence checks MUST maintain records of the checks carried out including copies of any evidence obtained to support the transactions / due diligence assessment. This is to meet the requirements of the Regulations and may be used as evidence in any subsequent investigation/inspection by the relevant supervising body.

9.2 The precise nature of the records is not prescribed by law; however, they must be capable of providing an audit trail during any subsequent investigation. For example distinguishing

the customer and the relevant transaction and recording in what form any funds were received or paid. In practice, the business units of the Council will be routinely making records of work carried out for customers in the course of normal business and these should suffice in this regard.

9.3 On **NO ACCOUNT** should a record of or any mention of, or, any referrals to, the Money Laundering Reporting Officer be kept / mentioned on a customer's file. The file must not contain details of any such suspicions as the file can be reviewed by the customer at any time and it is important that the customer is not "tipped off" about any allegations accidentally.

9.4 Records must be kept for a minimum of 5 years to allow for any investigation to take place.

9.5 A record of the destruction of such information (including the money laundering reporting form) must also be kept in line with normal Council procedures.

10. DATA PROTECTION CONSIDERATIONS

10.1 Regulation 41 of the MLR 2017 states that any personal data obtained by relevant persons for the purposes of these Regulations may only be processed for the purposes of preventing money laundering or terrorist financing.

10.2 In addition, new customers must be provided with the following information before establishing a business relationship or entering into an occasional transaction with the customer:

- the information specified in paragraph 2(3) of Part 2 of Schedule 1 to the Data Protection Act 1998 and
- a statement that any personal data received from the client will only be processed for the purposes of the preventing money laundering or terrorist financing unless permitted by an enactment or unless they provide consent.

10.3 Under data protection regulations any customer may ask to see the information held about them. This is called a Data Subject Access Request, and, under the law, this information must be provided. However, the regulations (both the General Data Protection Regulation and its predecessor) contain exemptions.

10.4 Exceptions apply in this case, where the release of the data would likely prejudice the prevention and detection of a crime or would cause the body releasing the information to actually commit a crime in doing so. As a result, money laundering referrals are usually exempt from any such subject access request, which is why the referral should not be documented on the customer's file. However, this does not prevent the release of all of the customer's information. Advice on the application of exemptions in this respect should be taken before any release of the information takes place.

11. RISK ASSESSMENT

11.1 Regulation 18 of the MLR 2017 requires the Council to identify, assess and manage the risk to council business in relation to Money Laundering.

11.2 This process is outlined in the corporate risk process framework and include:

- Identifying the money laundering and terrorist financing risks that are relevant to the Council;
- Assessing the risks presented by the particular customers, products and services, delivery channels and geographical area;
- Designing and implementing controls to manage and mitigate these assessed risks.

The risk assessment procedures and controls should be documented and kept under regular review.

11.3 The Council is also required to conduct ongoing monitoring of its business relationship in line with the risks which it has identified. This includes:

- Applying customer due diligence measures to verify the identity of customers and any beneficial owners obtaining additional information on customers,
- Conducting ongoing monitoring of the transactions and activity of customers with whom there is a business relationship,

11.4 Risks will be reviewed continuously as part of the annual review of the Council Risk Register.

11.5 For further advice or help in developing/considering money laundering risk contact the Head of Internal Audit, Anti-Fraud and Assurance.

12. TRAINING

12.1 Employees considered likely to be exposed to suspicious situations, will be made aware of these by their senior officer and provided with appropriate training.

12.2 Additionally, all employees and Members will be made aware of the legal and regulatory requirements relating to money laundering and terrorist financing, and the requirements of data protection, which are relevant to the implementation of the MLR 2017 and how they affect both the Council and themselves.

12.3 Notwithstanding the paragraphs above, it is the duty of employees and Members to report all suspicious transactions to the MLRO.

13. RELEVANT LEGISLATION

13.1 The following legislation is relevant to this policy:

- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017);
- Terrorism **Act** 2000;
- The Proceeds of Crime Act (POCA) 2002;
- Serious Crime Act 2015;
- Criminal Finances Act 2017

Appendix A

SUMMARY OF MONEY LAUNDERING OFFENCES THAT CAN BE COMMITTED

Proceeds of Crime Act 2002 – POCA
Money Laundering, Terrorise Financing and transfer of Funds (Information on the Payer) Regulations 2017 - MLR

Section Ref.	Type of Offence	Definition
S327 POCA	**Money Laundering Offence:** Concealing Criminal Property	A person commits an offence if they conceal, disguise, convert or transfer criminal property or if they remove criminal property from England, Wales, Scotland or Northern Ireland. This is punishable by a maximum term of imprisonment of 14 years at the Crown Court and an unlimited fine. At the Magistrates Court it is 6 months and £5,000 fine.
S328 POCA	**Money Laundering Offence:** Arrangements	This offence requires a person to become actively involved in some arrangement which helps someone else to get, keep, use or control the proceeds of a crime. The punishment is as for S327.
S329 POCA	**Money Laundering Offence:** Acquisition, Use and Possession	This offence is committed by anyone that has criminal proceeds in their possession provided they know or suspect that it represents the proceeds of a crime unless they paid 'adequate consideration' for it. Someone who pays less than the open market value is therefore guilty of the offence but someone who pays the full retail price, despite knowing or suspecting they are stolen goods is not guilty. The punishment is as for S327.
S330 POCA	**Failure to Disclose Offence:** Regulated Sector	This offence is committed by an employee of a business in the regulated sector who has knowledge or suspicion of another person's involvement in money laundering and does not make a report through the appropriate channels. Negligence is not a defence as the employee will be tried upon what they should have known given their experience, knowledge and training. This is punishable by a maximum term of imprisonment of 5 years and/or a fine.
S331 POCA	**Failure to disclose offence:** nominated officers in the regulated sector	This offence is committed by a nominated officer (MLRO) of a business in the regulated sector who has knowledge or suspicion of another person's involvement in money laundering and does not make a report through the appropriate channels without an acceptable excuse under the legislation. Negligence is not a defence as the nominated officer will be tried upon what they should have known given their experience, knowledge and training. The offence is triable either way with the same maximum penalty on indictment as an offence under section 330 (up to 5 years imprisonment).
S332	**Failure to Disclose**	This offence is committed by a nominated officer (MLRO) of a business

Section Ref.	Type of Offence	Definition
POCA	**Offence:** Other Nominated Officers	outside of the regulated sector who has knowledge or suspicion of another person's involvement in money laundering and does not make a report through the appropriate channels without an acceptable excuse under the legislation. The officer will be tried on what they knew or suspected not on what they might have been expected to know or suspect. This is punishable by a maximum term of imprisonment of 5 years and/or a fine.
S333 POCA	**Tipping Off Offence**	This offence is committed if an officer or Member makes a disclosure which is likely to prejudice an investigation being carried out by a law enforcing authority, knowing that such an investigation is in motion. This is punishable by a maximum term of imprisonment of 5 years and/or a fine.
Reg 86 MLR 2017	**Contravening a Relevant Requirement**	A person commits an offence if they have not followed any relevant guidance issued by the European Supervisory Authorities, Financial Conduct Authority or any other relevant supervisory authority approved by the Treasury. This is punishable by a maximum term of imprisonment of 2 years at the Crown Court, a fine, or both. At the Magistrates Court a term of three months, a fine, or both.
Reg 87 MLR 2017	**Prejudicing an Investigation**	This offence is committed when a person who knows or suspects that an appropriate officer is acting (or proposing to act) in connection with an investigation into potential contravention of a relevant requirement which is being or is about to be conducted. The offence is committed if either they make a disclosure which is likely to prejudice the investigation or they falsely, conceal, destroy or otherwise dispose of, or cause to permit the falsification, concealment, destruction or disposal of, documents which are relevant to the investigation. The punishment is as for Reg. 86 above.
Reg 88 MLR 2017	**Providing False or Misleading Information**	There are two separate offences under regulation 88. Under regulation 88(1) : a person commits an offence if: 1. In purported compliance with a requirement imposed on him by or under the MLR 2017, provides information which id false or misleading in a material particular and knows that the information is false or misleading; or 2. Is reckless as to whether the information is false or misleading. In respect of both offences, the punishment is the same as regs 86 and 87 above.

Appendix B

POSSIBLE SIGNS OF MONEY LAUNDERING

Criminals have various ways of concealing, moving and legitimising the proceeds of their crimes. This policy cannot list every potential scenario that could indicate money laundering however, some risk factors which *may*, either alone or along with other factors suggest the possibility of money laundering activity include:

General

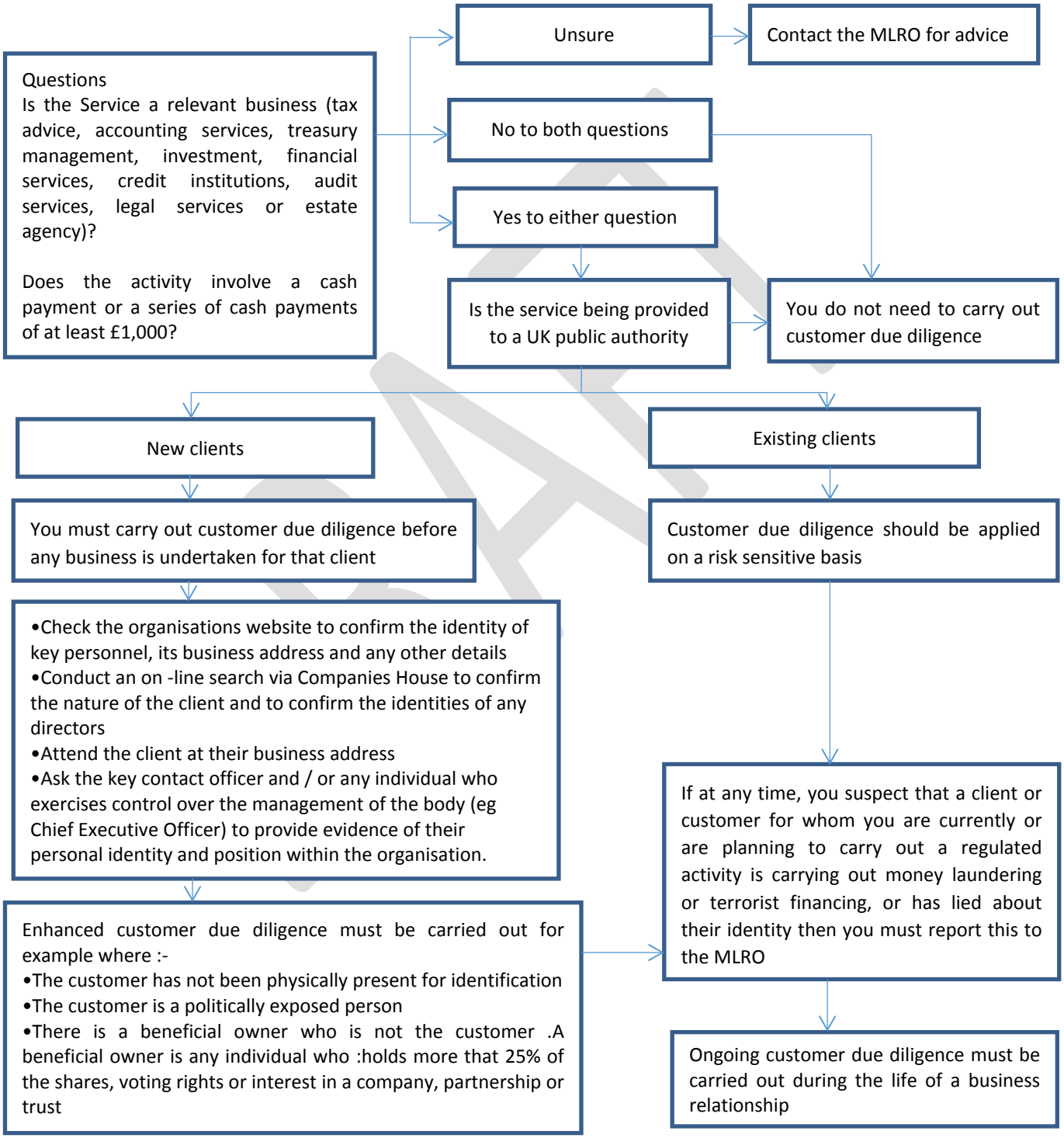
- A new customer with no previous 'history' with the Council;
- A secretive customer: for example, one who refuses to provide requested information without a reasonable explanation;
- Concerns about the honesty, integrity, identity of a customer;
- Illogical third party transactions: for example, unnecessary routing or receipt of funds from third parties or through third party accounts;
- Involvement of an unconnected third party in a transaction without logical reason or explanation;
- Payment of a substantial sum in cash (but it's reasonable to be suspicious of any cash payments particularly those over £1,000) where other means of payment are more normal (unusual transactions);
- Overpayments by a customer that are subsequently requested for a refund;
- Absence of an obvious legitimate source of the funds i.e. individuals of companies that appear insolvent (appear not to have funds) that are making transactions or are making transactions that appear beyond their means;
- Movement of funds to/from overseas, particularly to and from a higher risk country;
- Where, without reasonable explanation, the size, nature and frequency of transactions or instructions is out of line with normal expectations;
- A transaction without obvious legitimate purpose or which appears uneconomic, inefficient or irrational;
- Cancellation or reversal of an earlier transaction i.e. the payment of monies that are then requested back;
- Requests for release of customer account details other than in the normal course of business;
- Poor business records or internal accounting controls;
- A previous transaction for the same customer which has been, or should have been, reported to the MLRO.

Property Matters

- Unusual property investment transactions with no apparent investment purpose;
- Instructions to receive and pay out money where there is no linked substantive property transaction involved (surrogate banking);
- Regarding property transactions, funds received for deposits or prior to completion from an unexpected source or where instructions are given for settlement funds to be paid to an unexpected destination.

Appendix C

CUSTOMER DUE DILIGENCE PROCEDURE FLOWCHART



Appendix D

VERIFICATION OF CUSTOMER IDENTITY

Identity Verification Reference No: ……..……

NB: If you are receiving funds from a Council customer in any transaction **above £1,000 cash**, the identity of the person making the payment must be checked and confirmed.

All suspicions about possible Money Laundering, regardless of amount, should be reported to the Money Laundering Reporting Officer, via the Money Laundering reporting form.

CUSTOMER DETAILS

Forename		**Surname**	
Address			
Tel No (inc area code)		**Email Address**	
Payment in Respect of:		**Payment Reference**	
Amount	**£**	**Receipt Number** (If Applicable)	

If a payment is being made by a third party then please complete the details below in respect of the third party.

DETAILS OF THE THIRD PARTY MAKING THE PAYMENT:

Forename		**Surname**	
Address:			

A. EVIDENCE NOT OBTAINED – REASONS

1. Customer/third party previously identified in: Month ……Year ……

2. Other – state reason fully ……

B. EVIDENCE OBTAINED TO VERIFY INDIVIDUAL NAME AND ADDRESS

NB. <u>One</u> form of identification CANNOT be used to evidence <u>both</u> name and address.

For example, if a driving licence is provided as proof of name another form of identification must be provided to evidence an address, such as a utility bill.

PROOF OF IDENTITY CHECKLIST FOR INDIVIDUALS

Proof of name	**Proof of address**
Current signed passport	Utility bill (gas, electric, satellite television, landline phone bill) issued within the last three months
Original birth certificate (UK birth certificate issued within 12 months of the date of birth in full form including those issued by UK authorities overseas such as Embassies High Commissions and HM Forces)	Local authority council tax bill for the current council tax year
EEA member state identity card (which can also be used as evidence of address if it carries this)	Current UK driving licence (but only if not used for the name evidence)
Current UK or EEA photocard driving licence	Bank, Building Society or Credit Union statement or passbook dated within the last three months
Full old-style driving licence	Original mortgage statement from a recognised lender issued for the last full year
Photographic registration cards for self-employed individuals in the construction industry -CIS4	Solicitors letter within the last three months confirming recent house purchase or land registry confirmation of address
Benefit book or original notification letter from Benefits Agency	Council or housing association rent card or tenancy agreement for the current year
Firearms or shotgun certificate	Benefit book or original notification letter from Benefits Agency (but not if used as proof of name)
Residence permit issued by the Home Office to EEA nationals on sight of own country passport	HMRC self-assessment letters or tax demand dated within the current financial year
National identity card bearing a photograph of the applicant	Electoral Register entry
	NHS Medical card or letter of confirmation from GP's practice of registration with the surgery

NB. Documents unaccepted as evidence include, but are not limited to:

- Provisional driving licence
- Mobile phone bills
- Credit card statements

C. EVIDENCE OBTAINED FOR COMPANIES OR OTHER LEGAL STRUCTURES

Legal structure	**Corporate ID required**	**Individual ID required**

Legal structure	Corporate ID required	Individual ID required
A company (including a UK LLP)	Certificate of Incorporation or equivalent copy of filed audited accounts details of current company officers (i.e. directors and company secretary) and shareholders	Identity evidence for a) the individual dealing with the transaction and b) all other individuals or entities with 25% or more of the shares or voting rights in the company (see proof of identity checklist for individuals above)
A partnership with six or more partners	name of partnership trading address registered address (if any) nature of business recent audited accounts list of all partners list of all those with voting rights indicating their voting stake	Identity evidence for a) the partner responsible for the transaction and b) one other partner and c) all other individuals who (directly or indirectly) are entitled to, or control, 25% or more of the capital, profits or voting rights (see proof of identity checklist for individuals below)

D. DISADVANTAGED CUSTOMERS

E.g., Confirmation of identity from Social Worker or Bail Officer, Police, School, Courts etc.

E. If evidence not obtained for the reasons in A, do you have any suspicions regarding identity?

……..

I confirm that I have seen the originals of the documents indicated above and have identified the above Customer or Third Party.

Signed ……..…… Date ……

NB. Wherever possible TAKE COPIES of the identification evidence TO PLACE ON FILE. Copies should be notarised to indicate a copy and signed to evidence sight of the original.

Appendix E

CONFIDENTIAL

Report of Money Laundering Activity

To: Money Laundering Reporting Officer

From: …….
[Insert name of employee]

Directorate/Section: …… Ext/Tel No: ……
[Insert post title and Business Unit]

DETAILS OF SUSPECTED OFFENCE

Name(s) and address(es) of person(s) involved:
[if a company/public body please include details of nature of business]

Nature, whereabouts, value and timing of activity/property involved:
[Please include full details, e.g. what, when, where, how. Please also include details of current whereabouts of the laundered property, so far as you are aware. Continue on a separate sheet if necessary]

Nature of suspicions regarding such activity:
[Please continue on a separate sheet if necessary]

Has any investigation been undertaken (as far as you are aware)? Yes ☐ No ☐
[Please tick the relevant box]

If yes, please include details below:

Have you discussed your suspicions with anyone else? Yes ☐ No ☐
[Please tick the relevant box]

If yes, please specify below, explaining why such discussion was necessary:

Have you consulted any supervisory body guidance re money laundering? (e.g. the Law Society) Yes ☐ No ☐
[Please tick the relevant box]

If yes, please specify below:

Do you feel you have a reasonable excuse for not disclosing the matter to the NCA? (e.g. are you a lawyer and wish to claim legal professional privilege?) Yes ☐ No ☐
[Please tick the relevant box]

If yes, please set out full details below:

Are you involved in a transaction which might be a prohibited act (under section 327-329 of the Proceeds of Crime Act 2002 or Regulations 86-88 pf the MLR 2017 and which requires appropriate consent from the NCA? (refer to Appendix A – Money Laundering Offences) Yes ☐ No ☐
[Please tick the relevant box]

If yes, please set out full details below:

Please set out below any other information you feel is relevant:

Signed: …… Dated: ……

Please do not discuss the content of this report with anyone else and <u>in particular</u> 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.

THE FOLLOWING PART OF THIS FORM IS FOR COMPLETION BY THE MLRO

Date report received: ……

Date receipt of report acknowledged: ……..

CONSIDERATION OF DISCLOSURE:

Action plan:

OUTCOME OF CONSIDERATION OF DISCLOSURE:

Are there reasonable grounds for suspecting money laundering activity?

If there are reasonable grounds for suspicion, will a report be made to the NCA? Yes ☐ No ☐
[Please tick the relevant box]

If yes, please confirm date of report to the NCA: ……...
And complete the box below:

Details of liaison with the NCA regarding the report:
Notice Period: ……..……. **To** ……..…….
Moratorium Period: …….. **To** ……

Is consent required from the NCA to any ongoing or imminent transactions which otherwise be prohibited acts [Please tick the relevant box]	**Yes** ☐	**No** ☐

If yes, please confirm full details in the box below:

Date consent received from the NCA: **……..……**

Date consent given by you to employee: **……..……..**

If there are reasonable grounds to suspect money laundering, but you do not intend to report the matter to SOCA, please set out below the reason(s) for non-disclosure:

[Please set out any reasonable excuse for non-disclosure]

Date consent given by you to employee for any prohibited act transactions to proceed: **……..……**

Other relevant information:

Signed: …… Date: ……

THIS REPORT TO BE RETAINED SECURELY FOR AT LEAST FIVE YEARS

Earliest disposal date: ……