APPENDIX 2

Tameside Metropolitan Borough

Anti-Money Laundering Policy

December 2023

Contents

Anti-Money Laundering Policy

1. INTRODUCTION

1.1 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.

1.2 Although Local Authorities are not directly covered by the requirements of The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, guidance from the Chartered Institute of Public Finance and Accountancy ("CIPFA") indicates that they should comply with the underlying spirit of the legislation and regulations.

1.3 Tameside Metropolitan Borough 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.

1.4 This policy should be read in conjunction with the Council's Counter Fraud Policy & Strategy and the Councils Whistleblowing 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. A breach of this Policy may lead to disciplinary and/or criminal action being taken.

2. SCOPE

2.1 This policy applies to Tameside Metropolitan Borough Council, and as a consequence it applies to all its members and all employees, including temporary and agency staff. It contains specific sections to advise employees and members of the process to be followed to enable the Council to comply with its legal obligations.

2.2 Our policy is to ensure all appropriate action is taken to prevent, wherever possible, the Council and its members and employees from being exposed to money laundering and to comply with all legal and regulatory obligations, including the reporting of suspected or actual cases in line with disclosure requirements.

3. MONEY LAUNDERING

3.1 The Proceeds of Crime Act 2002 (as amended by the Crime and Courts Act 2013, Serious Crime Act 2015 and the Criminal Finances Act 2017), Terrorism Act 2000 (as amended by the Criminal Finances Act 2017) and the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (as amended by the Money Laundering and Terrorist Financing (amendment) Regulations 2019) cover a range of activities and offences in relation to money laundering. The

primary ones are listed below; further details are provided in **Appendix A: Offences Table:**

- Concealing, disguising, converting, or transferring criminal property or removing it from the UK; (section 327 of the 2002 Act); or
- 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; (section 328); or
- Acquiring, using or possessing criminal property; (section 329);
- Failure to disclose knowledge or suspicion of another person(s) involvement in money laundering; and,
- Tipping off 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.

3.2 These offences cover a range of activities, which do not necessarily need to involve 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 activity, irrespective of the size of the benefit gained, and/or fail to report their concerns.

3.3 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.

3.4 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. 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 in **Appendix B: Possible Signs of Money Laundering.**

3.5 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; then they may be liable to prosecution. Heavy penalties, including unlimited fines and up to 14 years imprisonment, can be handed down to those who are convicted of one of the offences listed in paragraph 3.1 above.

3.6 The key requirement for Council employees, members, and partners, is to promptly report any suspected money laundering activity to the Council's Head of Assurance, who fulfils the role of the Money Laundering Reporting Officer (MLRO), (POCA, Section 337, Protected Disclosures).

4. REQUIREMENTS OF THE MONEY LAUNDERING LEGISLATION

4.1 The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 impose 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 (£12,000) or more.

4.3 Some activities undertaken by the Council could be included within the scope of the money laundering regulations. Therefore, to ensure compliance with the regulations and legislation and for the purposes of this Policy, the Council are considered a relevant person when acting in the course of business and activities carried on by them.

4.4 The obligations include the following requirements:

- Appoint a 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 five years).

4.5 The European Union 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 Senior Management should maintain engagement with Risk Management and Audit Services 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 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 (NCA).

5.2 The Council's nominated MLRO is: Head of Assurance

Address: Tameside One, Market Place, Ashton-under-Lyne, Tameside, OL6 6BH

Telephone: 0161 342 3231

5.3 In the absence of the MLRO or in instances where it is suspected that the MLRO is involved in suspicious transactions, concerns should be raised with the Audit Manager

Address: Tameside One, Market Place, Ashton-under-Lyne, Tameside, OL6 6BH

Telephone: 0161 342 2870

5.4 Or, please refer to the Whistleblowing Policy.

6. DUE DILIGENCE PROCEDURE

6.1 Where the Council is carrying out activities in the course of business (see paragraph 4.2 above), extra care needs to be taken to check the identity of the customer – this is known as carrying out customer due diligence. This is covered in Regulations 27-38 of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. Details of the process to be undertaken is provided in **Appendix C: Customer Due Diligence Procedure Flowchart**.

6.2 The requirement for customer due diligence applies immediately for new customers and should be applied on a risk basis for existing customers. Ongoing customer due diligence must also be carried out during the life of a business relationship but should be proportionate to the risk of money laundering and terrorist funding, based on the officers' knowledge of the customer and a regular scrutiny of the transactions involved.

6.3 Due diligence essentially means identifying the customer and verifying their identity on the basis of documents. Data or information obtained from reliable and independent source and depending upon the purpose and intended nature of the business relationship. Where you need to carry out customer due diligence then you must seek evidence of identity. See **Appendix D: Verification of Customer Identity**.

6.4 Where the customer is acting or appears to be acting for someone else, reasonable steps must also be taken to establish the identity of that other person.

Payments

6.5 Where cash in excess £1,000 is received from customers, employees should ask for, and inspect, identification. See **Appendix D: Verification of Customer Identity**. This will help to identify and report any suspicious transactions.

6.6 Electronic or cheque payments to the Council are easily traceable through the banking system. As traceability is key and an individual walking in to pay a debt with cash is not necessarily traceable, it is best practice to recommend on payment electronically from a UK Clearing Bank.

6.7 An upper limit of €10,000 (which is currently the equivalent to approximately £9000) should be set for cash transactions. Even though the regulations do not apply to Local Authorities it is recommended that an upper limit be established for cash payments which include notes, coins or travellers cheques in any currency. If a larger sum in cash is offered this needs to be referred to the MLRO for consideration.

6.8 Overpayments made via credit card, debit card, standing order or direct debit, should only be refunded by crediting the overpayment to the card or bank account which made the original payment.

General

6.9 In general:

- The Council knows most of its customers and those through whom they are acting – there is no, or very little, doubt as to their identity;
- Any Services that may be defined as regulated business activities are provided to customers who are UK Local Authority/Public Bodies; and

- The Council is subjected to defined, robust public sector governance and financial management controls.

Record Keeping Procedures

6.10 Each area of the Council acting in the course of business carried out by them, see paragraph 4.2 above, must maintain due diligence records, preferably electronically, and details of all relevant transactions carried out for customers for a minimum of five years from the date of (as appropriate) the transaction/end of any client relationship. This is to meet the requirements of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (Regulation 4) and may be used as evidence in any subsequent investigation/inspection by the relevant supervising body.

6.11 Records must be capable of providing an audit trail during any 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 areas of the Council will be routinely maintaining such records in the course of normal business and these should suffice in this regard.

6.12 Any record keeping should be in line with GDPR and the originating Service Areas Privacy Statement.

7. POLITICALLY EXPOSED PERSON

7.1 A Politically Exposed Person is defined, in the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, as "an individual who is entrusted with prominent public functions, other than as a middle-ranking or more junior official."

7.2 The Council must determine whether a customer or the beneficial owner of a customer is:

a) a politically exposed person (a PEP); or
b) a family member (including spouse, civil partner, children, parents), or a known close associate (such as sole or joint beneficial ownership of a legal entity) of a PEP.

and manage the enhanced risks arising from the relevant person's business relationship or transactions with such a customer.

7.3 Where an employee has determined that a customer, or a potential customer, is a PEP, or a family member or known close associate of a PEP, the relevant person must assess;

(a) the level of risk associated with that customer, and

(b) the extent of the enhanced due diligence measures to be applied in relation to that customer.

7.4 Where the Council proposes to have, or to continue, a business relationship with a PEP, or a family member or a known close associate of a PEP, the Council must:

(a) have approval from senior management for establishing or continuing the business relationship with that person;

(b) take adequate measures to establish the source of wealth and source of funds which are involved in the proposed business relationship or transaction with that person; and

(c) where the business relationship is entered into, conduct enhanced ongoing monitoring of the business relationship with that person.

8. REPORTING PROCEDURE FOR SUSPICIONS OF MONEY LAUNDERING

8.1 Where an employee or member knows or suspects that money laundering activity is taking place (or has happened) they must immediately disclose to the MLRO. If the employee or member does not immediately report this to the MLRO then they may be liable to prosecution. Examples of warnings signs or relevant Council activity of possible money laundering are listed in Appendix B.

8.2 Disclosure should be made to the MLRO in line with the procedure outlined at **Appendix E: Suspicious Transactions Reporting Procedure**. The standard pro-forma report attached at **Appendix F: Money Laundering Disclosure Report** should be used for this purpose. 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 B: Possible Signs of Money Laundering**);
- 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 judgement 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.

8.3 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 Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 see **Appendix A: Offences Table**, then the report must include 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.

8.4 Employees and members must still report concerns, even if it is believed someone else has already reported their suspicions of the same money laundering activity.

8.5 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. At no time, and under no circumstances, should an employee voice any suspicions to the person(s) whom is suspected of money laundering, otherwise they may commit a criminal offence of “tipping off”. However, preliminary enquiries of a client to obtain more

information (e.g. to confirm their identity, clarify the source of funds) will not constitute tipping off unless the employee knows or suspects that a report has been made.

8.6 Should allegations be raised regarding employees of the Council then the Councils Disciplinary Procedure will also apply.

8.7 Should the allegations be raised regarding members of the Council then the Head of Democratic Services should also be contacted.

8.8 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 for prosecution. The MLRO must keep the appropriate records in a confidential manner.

8.9 Any information containing personal and/or sensitive data which is supplied or processed during the course of a money laundering investigation shall not be processed wider than is absolutely necessary for the purposes of determining whether a money laundering offence has been committed.

9. ACTION BY THE MONEY LAUNDERING REPORTING OFFICER

9.1 The MLRO must promptly evaluate any Disclosure Report, in the light of relevant information which is available and determine whether it gives rise to knowledge or suspicion, or reasonable grounds for knowledge or suspicion, that a person is engaged in money laundering or terrorist financing, to determine whether it should be reported to the NCA. The MLRO will notify the Statutory Monitoring Officer before any reports are made to the Police or the NCA.

9.2 The MLRO must normally suspend the transaction if they suspect money laundering or terrorist financing. If it's not practical - or not safe - to suspend the transaction, they should make the report as soon as possible after the transaction is completed.

9.3 Once the MLRO has evaluated the Disclosure Report they must make a timely determination as to;

- whether there is, or seems to be, any evidence of money laundering or terrorist financing taking place;
- whether consent needs to sought from the NCA for a particular transaction to proceed.

9.4 If the MLRO determines actual or suspected money laundering activity then, with advice from the Statutory Monitoring Officer, this should be promptly reported to the NCA. This can be done online using the SAR Online System, see link below, which will provide instant acknowledgement and a reference number.

https://www.ukciu.gov.uk/saronline

Alternatively paper forms can be obtained from:

http://www.nationalcrimeagency.gov.uk/crime-threats-sars

9.5 The MLRO commits a criminal offence if he/she knows or suspects, or has reasonable grounds to do so, through a disclosure being made to her, that another person is engaged in money laundering and does not disclose this as soon as practicable to the NCA.

9.6 All Disclosure Reports referred to the MLRO and reports made by the MLRO to the NCA must be retained by the MLRO in a confidential file kept for that purpose and retained for a minimum of six years. A copy of the Disclosure Report must be provided to the Council's Statutory Monitoring Officer.

10. TRAINING AND AWARENESS

10.1 The Council will provide all employees and members with fraud awareness training which will cover the law relating to money laundering and terrorist financing and transfer of funds.

10.2 The Council may provide additional service specific training to areas that post a higher risk to attempts to launder money.

10.3 Notwithstanding the paragraphs above, it is the duty of employees and members to report all suspicious transactions whether they have received their training or not.

10.4 Further information can be obtained from the MLRO and the following sources;

- National Crime Agency Home - National Crime Agency
- CIPFA Home (cipfa.org)
- CCAB - Anti money laundering (proceeds of crime and terrorism) guidance for accountants Anti-Money Laundering and Counter-Terrorist Financing Guidance for the Accountancy Sector 2020 - CCAB
- The law society - Anti-money laundering guidance and advice Anti-money laundering | The Law Society
- Other relevant council policies.

11. REVIEW

11.1 This policy will be reviewed on an annual basis.

APPENDIX A

OFFENCES TABLE

Section Ref.	Type of Offence	Definition
S327 Proceeds of Crime Act 2002	**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 a £5,000 fine.
S328 Proceeds of Crime Act 2002	**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 Proceeds of Crime Act 2002	**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 Proceeds of Crime Act 2002	**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.

Section Ref.	Type of Offence	Definition
S331 Proceeds of Crime Act 2002	**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. This is punishable by a maximum term of imprisonment of 5 years and/or a fine.
S332 Proceeds of Crime Act 2002	**Failure to Disclose Offence:** Other Nominated Officers	This offence is committed by a nominated officer (MLRO) of a business 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.
S332 Proceeds of Crime Act 2002	**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 Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 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.

Section Ref.	Type of Offence	Definition
Reg 87 Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017	**Prejudicing and 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.
Reg 88 Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 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 is 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

Types of risk factors which *may*, either alone or along with other factors, suggest the possibility of money laundering activity:

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 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 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 above £1,000);
- Overpayments by a customer;
- Absence of an obvious legitimate source of the funds;
- 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 to irrational;
- Cancellation or reversal of an earlier transaction;
- 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.
- A refund request following the cancellation or reversal of an earlier transaction;
- A person suddenly changes their pattern of activity i.e. if someone is usually in arrears and then they pay off the arrears and pay a large sum in advance;
- A customer's profile does not fit the transaction, i.e. a person enters into an arrangement beyond their apparent financial means;
- A customer attempts to use cash to complete a proposed transaction when this type of business transaction would normally be handled by card payment or an electronic payment;
- The source or destination of funds (such as a refund) differs from the original details given by the client;
- Cash paid exceeds the amount necessary to settle a transaction and a non-cash return of the excess is requested.

PROPERTY MATTERS

- The other party is happy to enter into an apparent bad deal for them and is not interested in obtaining a better price for the transaction;
- A developer/third party offers the Council a price for land/property that is far in excess of its estimated value;
- Unusual property investment transactions if there is no apparent investment purpose or rationale;
- There is an unexplained and unusual geographic use of a solicitor in relation to a purchase of a property/parcel of land;
- Where there is more than one solicitor/conveyancer used in the sale or purchase of a property or land;
- Funds received for deposits, or prior to completion, from an unexpected source or where instructions are given for settlement funds
- If the buyer or seller's financial profile does not fit.

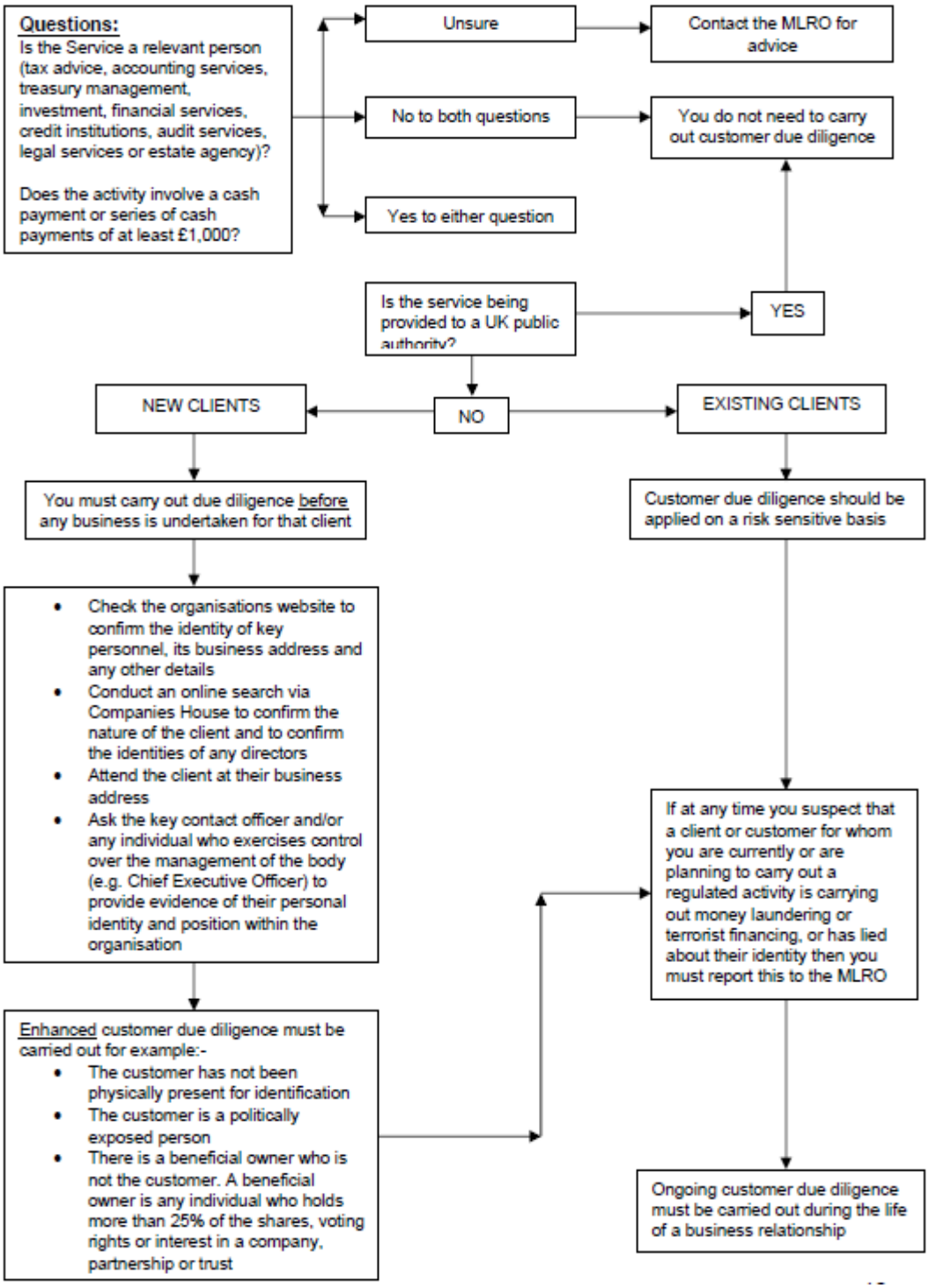
The following table sets out the types of activities that might be suspicious and where the Council may be susceptible to money laundering activities. It is not intended to be exhaustive, and just because something is not on the list, it doesn't mean that it should not be reported.

ACTIVITY	The types of activity that may be affected
New customers with high value transactions	Selling property to individuals or businesses. Renting out property to individuals or businesses. Entering into lease agreements.
Secretive clients	Housing benefit claimants who have sums of money entering into/out of their bank account (even if we do not award them benefit, we should still consider money laundering implications). People buying or renting property from the Council who may not want to say what it is for. People receiving grant funding who refuse to demonstrate what the funding was used for.
Customers who we think are acting dishonestly or illegally	People paying for Council services who do not provide details about themselves. People making odd or unusual requests for payment arrangements.
Illogical transactions	People paying in cash then requesting refunds. Requests for the Council to pay seemingly unconnected third parties in respect of goods/services provided to the Council. Requests for the Council to pay foreign currencies for no apparent reason.

ACTIVITY	The types of activity that may be affected
Payments of substantial sums by cash	Large debt arrears paid in cash. Refunding overpayments. Deposits/payments for property.
Movement of funds overseas	Requests to pay monies overseas, potentially for “tax purposes”.
Cancellation of earlier transactions	Third party “refunds” grant payment as no longer needed/used. No payment demanded even though goods/services have been provided. Sudden and unexpected termination of lease agreements.
Request for client account details outside normal course of business	Queries from other companies regarding legitimacy of customers. Council receiving correspondence/information on behalf of other companies.
Extensive and over-complicated client business structures / arrangements	Requests to pay third parties in respect of goods/services. Receipt of business payments (rent, business rates) in settlement from seemingly unconnected third parties.
Poor accounting records and internal financial control	Requests for grant funding/business support indicates third party is not supported by financial information. Companies tendering for contracts unable to provide proper financial information/information provided raises concerns. Tender for a contract which is suspiciously low
Unusual property investment or transactions	Requests to purchase Council assets/land with no apparent purpose. Requests to rent Council property with no apparent business motive.
Overcomplicated legal arrangements/multiple solicitors	Property transactions where the Council is dealing with several different parties.

APPENDIX C

CUSTOMER DUE DILIGENCE PROCEDURE FLOWCHART



APPENDIX D

VERIFICIATION OF CUSTOMER IDENTITY

Verification of Customer Identity Checklist for customer:

Name:

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

All suspicions, regardless of amount, should be reported to the MLRO via the Money Laundering Reporting Form.

A. Evidence not obtained – reasons:

1. Customer previously identified in: Month: --- Year: ---

2. Other - state reason fully:

B. Evidence obtained to verify name and address:

(GROUP A) – Acceptable on their own:

- Full National Passport.
- Full National Driving Licence with photo.
- Pension book.
- Armed Forces ID Card.
- Signed ID card of employer known to you.

(GROUP B) – Acceptable with two of next group below:

- Young person NI Card (under 18 only).
- Pensioner's travel pass.
- Building Society passbook.
- Credit Reference agency search.
- National ID card.
- Copy Company Certificate of Incorporation if a Limited Company.
- Company and 2 Directors personal identity as above.

(GROUP C) - *NOT acceptable on their own:

- Gas, electricity, telephone bill.
- Mortgage statement.
- Council Tax demand.
- Bank/Building Society/Credit Card Statement.
- Young person's Medical Card (under 18 only).
- Home visit to applicants address.
- Check of telephone directory.
- Check electoral roll.

**Suitable for proof of address only*

NB BEST PRACTICE is to have one of Group A plus two of Group C.

C. Evidence obtained for unquoted company or partnership:

- Certificate of Incorporation or equivalent.
- Certificate of Trade or equivalent.
- Latest report and audited accounts.
- Principal shareholder/partner (personal ID).
- Principal Director (personal ID).
- Screenshot of the customer's website to confirm their business address.
- Screenshot of Companies House website detailing the nature and business of the customer and confirming the identities of Directors.
- A written instruction on the organisation in question's headed paper.

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(s)

Signed:

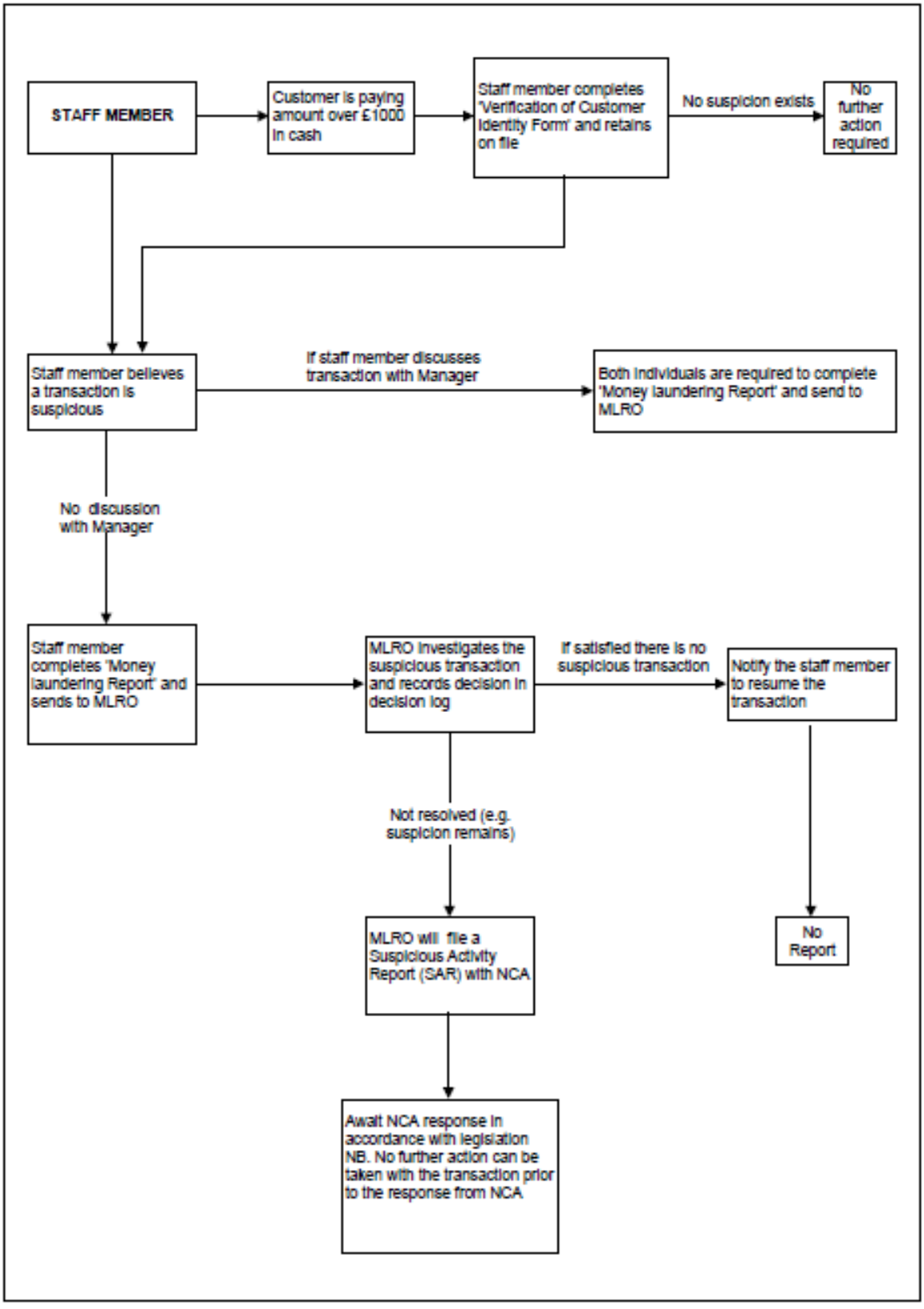
Date:

NB Wherever possible take copies of the identification TO RETAIN ON FILE. Copies should be notarised to indicate a copy and signed to evidence sight of the original.

Where a client's identity has been confirmed under the client verification procedure the record of evidence obtained must be retained for at least six years. In practice, such evidence will be obtained in the normal course of business and this should be sufficient for this requirement.

APPENDIX E

SUSPICIOUS TRANSACTION REPORTING PROCEDURE



APPENDIX F

CONFIDENTIAL

MONEY LAUNDERING DISCLOSURE REPORT

To: **Money Laundering Reporting Officer**

From:

(*Insert name of officer)*

Service Area /Post Title: ---

Tel No: ---

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, value, and timing of activity involved:
(Please include full details e.g. what, when, where, how. 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

If yes, please include details below:

Have you discussed your suspicions with anyone else? Yes / No

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

Have you consulted any supervisory body guidance re money laundering? Yes / No (e.g. the Law Society)

If yes, please specify below:

Do you feel you have a reasonable excuse for not disclosing the matter to the National Crime Agency? (e.g. are you a lawyer and wish to claim legal professional privilege?) Yes / No

If yes, please set out full details below:

Are you involved in a transaction that might be a prohibited act under sections 327- 329 of the Proceeds of Crime Act 2002 or Regulations 86 – 88 of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 and which requires appropriate consent from the National Crime Agency? See Appendix A, Offences Table) Yes / No

If yes, please enclose details in the box 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 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 National Crime Agency? Yes / No

In accordance with Council Policy the Statutory Monitoring Officer should authorise referrals to the Police/National Crime Agency. Please confirm authorisation.

If yes, please confirm the date of the report to the National Crime Agency:
and complete the box below:

Date:

Details of liaison with National Crime Agency regarding the report:

Notice of Period: ---------- to ----------

Moratorium Period: ---------- to ----------

Is consent required from National Crime Agency to any on-going or imminent transactions which would otherwise be prohibited acts? Yes / No

If yes, please confirm full details below:

Date consent received from National Crime Agency: ……

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 National Crime Agency please set out below the reason(s) for non-disclosure:

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

Other relevant information:

Signed:

Dated:

Copied to Statutory Monitoring Officer

CONFIDENTIAL

Acknowledgment of Receipt of Report

Dear _____

Thank you for your recent money laundering suspicion report. I have logged this in my file and allocated it a unique reference number _____

You must not continue with any further business or execute any transactions, on behalf of this client without my consent.

In the meantime, please remember not to discuss your report, or the fact that you have made a report, with anyone except me. In particular, do not indicate in any way to the client that a report has been made about him or record such information on the client file.

If I need any more information, I will get in touch with you. If you are concerned about the report or about dealing with the client in the future, please contact me to discuss it.

If other people within our organisation need to know about the report, I will let them know.

Yours sincerely

Money Laundering Reporting Officer

Copied to Statutory Monitoring Officer

CONFIDENTIAL

Money Laundering Consent to Proceed Form

DETAILS OF MLRO

Name

(*Insert name of MLRO/Authorised Deputy)*

Position Tel No:

--- ---

(*insert post title)*

DETAILS OF EMPLOYEE / MEMBER

Name

(*Insert name of employee / member)*

Position/
Directorate Ext/Tel No:

--- ---

(*insert post title/directorate)*

DETAILS OF REPORT

Report unique number

Date of report

OUTCOME

I can confirm that the above transaction/query can proceed

Signed ……. Date ……

(*MLRO/Authorised Deputy)*

Copied to Statutory Monitoring Officer