



Anti-Money Laundering Policy Statement and Strategy

September 2022



Contents

	Page No
1. Introduction and Scope	1
2. What is money laundering	2
3. Obligations on the council	4
4. The money laundering reporting officer (MLRO)	5
5. Reporting to the MLRO	5
6. Responsibility of the MLRO/DMLRO	5
7. Customer due diligence	7
8. Internal clients	9
9. External clients	9
10. Simplified due diligence	9
11. Enhanced customer due diligence and ongoing monitoring	10
12. Red flag indicators	11
13. Record keeping	11
14. Training and staff awareness	12
15. Risk management and internal control	12
16. Version Control	12
Appendix A	13
Appendix B	17
Appendix C	20
Appendix D	22
	23



1. Introduction and Scope

- 1.1 The Money Laundering and Terrorist Financing Regulations 2019 (MLR 2019) came into force on the 10 January 2020. The new Regulations widen the scope of the regulated sector from that defined by the 2017 Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations (MLR 2017), which came into force on 26 June 2017.
- 1.2 This policy explains what money laundering is and outlines the council's commitment to comply with the MLR 2019. It sets out the procedures and governance frameworks that must be followed (for example the reporting of any suspicions of money laundering activity) to enable the council to comply with its legal obligation to prevent and detect money laundering.
- 1.3 Local authorities are not directly covered by the requirements of MLR 2019, however, the consensus among financial and legal regulators/institutions (including the Chartered Institute of Public Finance and Accounting [CIPFA]), is that all public service organisations should comply with the underlying spirit of MLR 2019 and put in place appropriate and proportionate safeguards and reporting arrangements.
- 1.4 The MLR 2019 imposes specific obligations on “relevant persons”. 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 £12,000 (€15,000) or more.
- 1.5 Not all the council business would fall under the definition of “relevant”, however, the safest way to ensure compliance with the law is to apply the definition of "relevant" to all areas of work undertaken by the council.
- 1.6 This policy therefore applies to all employees and elected members of Lancashire County Council. The definition of employee includes casual/temporary employees, agency staff and any contractor acting on behalf of the council. The council will ensure its partners and all companies it is in contract with are informed of the procedures the council has in place to tackle money laundering.
- 1.7 This policy forms part of the council's wider commitment to tackle all forms of Financial Crime and should be read in conjunction with the council's counter-fraud strategy, anti-bribery and corruption, and whistleblowing policies.



2. What is money laundering

2.1 Money laundering in simple terms is a process that makes money with an illegal origin appear legal, or simply put to make "bad money appear good". The ultimate aim of a money launderer is to legitimise the criminal funds so they can spend it in the mainstream wider economy without drawing the attention of law enforcement agencies to the original criminality.

2.2 Money laundering often involves 3 steps:

- **Placement** – cash is introduced into the financial system by some means;
- **Layering** – a single or series of transactions to camouflage the illegal source;
- **Integration** – the funds are reintroduced into the economy to appear legitimate, e.g., receiving an item, property, money or service in return.

2.3 Money launderers are often intuitive and come across as very plausible in how they operate/present themselves. They can use complex "cover stories" or even businesses to enable their activity and disguise their criminal intent. Their true motive is to establish a relationship with a legitimate business or large institution and use them to unwittingly "clean" their criminal funds. This exposes the council to the risk of being targeted by criminals.

2.4 Money laundering is a term used to describe several different offences that involve the proceeds of crime or terrorism funds. money laundering is defined as (further details in **Appendix A**):

- concealing, disguising, converting, transferring criminal property, or removing it from the UK; 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; or
- acquiring, using, or possessing criminal property.
- 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.

2.5 Money laundering is included within the following pieces of legislation:

- Proceeds of Crime Act 2002 (the POCA) (as amended by the Serious Organised Crime and Police Act 2005, Crime and Courts Act 2012, Serious Crime Act 2015 and Criminal Finances Act 2017).



- Money Laundering Terrorist Financing & Transfer of Funds (Information on the Payer) Regulations 2017 (as amended by the money laundering & Terrorist Financing (amendment) Regulations 2019).
- The Terrorism Act 2000 (as amended by the Criminal Finances Act 2017).
- Offences under the Bribery Act 2010 may also constitute money laundering.

2.6 The legislation covers all criminal property where the alleged offender knows or suspects the property constitutes or represents benefit from any criminal conduct. Property is all property (including tax evasion) situated anywhere in the world for example:

- Money
- All real, personal, heritable or 'moveable property'
- Intangible and incorporeal property
- Property obtained by a person who has an interest in it
- Things in action and other intangible or incorporeal property

2.7 Whilst the risk to the council of contravening the legislation is low, it is extremely important that all employees are familiar with their legal responsibilities: serious criminal sanctions may be imposed for breaches of the legislation. **The key requirement on employees is to promptly report any suspected money laundering activity to the Money Laundering Reporting Officer (MLRO) or Deputy MLRO (as detailed in section 5 below).**

2.8 It is impossible to give a definitive list of ways to spot money laundering or how to decide whether you need to make a report. Facts or just a gut instinct that something isn't quite right, can all lead you to the conclusion that you must report your concern. The law says this intangible feeling can be deemed sufficient to form a reasonable suspicion of money laundering. It is therefore important that in these circumstances you report your concerns. Failure to do so could lead to you committing an offence. Risk factors can either alone or cumulatively with other factors, suggest the possibility of money laundering activity and these are provided at **Appendix B: Possible signs of money laundering.**

2.9 It is important to understand that when an employee suspects money laundering (and reports it in line with this policy), or when an employee is aware that someone else has reported a concern in line with this policy, they must exercise caution in what is discussed with others, as this may be captured under the further offence of tipping off should it potentially prejudicing an investigation. The offence of tipping off is taken very seriously by law enforcement and any employee who falls into this scenario could be subject to criminal prosecution. For this reason,



it is strongly advised that employees refrain from talking to others about the suspicion/report and avoid engaging in gossip or reckless conversation.

3. Obligations on the council

- 3.1 Not all the council's business is "relevant" for the purposes of MLR 2019. It is mainly accountancy, financial, company and property transactions that are deemed relevant.
- 3.2 The obligations on the council are to establish and maintain appropriate and risk-sensitive policies and procedures. The council must:
- Appoint a money laundering reporting officer (MLRO) to receive disclosures of money laundering activity;
 - Implement a procedure to enable reporting of suspicions of money laundering;
 - Apply due diligence measures in certain circumstances;
 - Know the intended nature of business relationships and undertake ongoing monitoring of them (to identify unusual transactions);
 - Maintain client identification procedures in certain circumstances;
 - Maintain record keeping procedures retaining details of transactions for at least 5 years;
 - Conduct money laundering and terrorist funding risk assessment and adopt appropriate internal controls; and
 - Train relevant staff.

4. The Money Laundering Reporting Officer (MLRO)

- 4.1 The MLRO for Lancashire County Council is designated as N.Kissock, Director of Finance. The Deputy MLRO (DMLRO) for Lancashire County Council is designated as P.Walker, Senior Investigator, who is authorised to deputise for the MLRO. The MLRO delegates responsibility for receiving, reviewing and reporting on suspected money laundering to the DMLRO. The MLRO and DMLRO can be contacted at MLRO@lancashire.gov.uk
- 4.2 The DMLRO will report monthly to the MLRO in relation to the money laundering landscape across the council and the MLRO will report annually to the Audit, Risk and Governance Committee on this matter if applicable.



5. Reporting to the MLRO

- 5.1 Any employee who suspects money laundering activity is taking place must report/disclose this promptly in line with this policy. This includes when an employee becomes concerned that their involvement in a matter may amount to a prohibited act under the legislation.
- 5.2 The disclosure should be made using the proforma attached as **Appendix C**. As much detail as possible should be included in the report. This must be emailed to MLRO@Lancashire.gov.uk.
- 5.3 The employee **MUST** follow any subsequent directions from the MLRO/DMLRO and must **NOT** make any further enquiries themselves into the matter. It is important the employee takes no further steps in the transaction without authorisation from the MLRO/DMLRO. The MLRO/DMLRO may need to obtain consent from the National Crime Agency (NCA) before the transaction can proceed. If an employee was to allow the transaction to proceed without the MLRO/DMLRO authorisation, then the employee would be in breach of the legislation.
- 5.4 The employee must not disclose or otherwise indicate their suspicions to the person(s) suspected of money laundering. They must not discuss the matter with others. They should refrain from putting any form of notes on a file that a report has been made as this could result in the suspect becoming aware of the concern. Please remember this could constitute the offence of tipping off.

6. Responsibility of MLRO/DMLRO

- 6.1 The DMLRO will acknowledge receipt of the disclosure and will promptly evaluate the information to determine whether it is appropriate to report it to the National Crime Agency. The DMLRO will also provide you with a predicted timescale for a response to your disclosure.
- 6.2 The DMLRO will consider the report and other available internal material deemed relevant for example:
 - Reviewing other transaction patterns and volumes
 - The length of any business relationship involved
 - The number of any on-off transactions and linked one off transactions
 - Any identification evidence held
- 6.3 The DMLRO will undertake such other reasonable enquiries they think is appropriate in order to ensure that all available information is considered when deciding whether a report to the



National Crime Agency (NCA) is required. The DMLRO may also need to discuss the report with you for further information.

- 6.4 Once the DMLRO has evaluated the disclosure report and any other relevant information, they must make a timely determination as to whether:
- There is actual or suspected money laundering taking place;
 - There are reasonable grounds to know or suspect that is the case;
 - They know the identity of the money launderer or the whereabouts of the property involved, or they could be identified or the information may assist in such Identification; and
 - Whether the DMLRO needs to seek consent from the NCA for a particular transaction to proceed.
- 6.5 The DMLRO will promptly report the matter to the NCA through the NCA website if they have concluded it meets the criteria of submitting a Suspicious Activity Report (SAR). The DMLRO is registered with the NCA and will log-in to submit any report themselves. This is likely to be done in liaison with the person raising the concern.
- 6.6 When the DMLRO concludes that there are no reasonable grounds to suspect money laundering then consent will be given for any ongoing or imminent transactions to proceed. The reasons will be recorded on the AML log and disclosure form.
- 6.7 All disclosure reports referred to the MLRO/DMLRO and reports made to the NCA by the DMLRO will be stored in a confidential file kept for that purpose for a minimum of 6 years.
- 6.8 If the DMLRO concludes that a matter meets the criteria of submitting a SAR, the DMLRO must disclose the matter as soon as practicable to the NCA unless they have a reasonable excuse for non-disclosure to the national crime agency (e.g., if you are a lawyer and wish to claim legal professional privilege for not disclosing the information).
- 6.9 In such a scenario where a solicitor is claiming legal professional privilege (LPP), a joint decision will be made between the MLRO/DMLRO and the solicitor to agree if the LPP exemption applies. In the very unlikely event a consensus decision is not met. The MLRO/DMLRO will consult with the Director of Corporate Services to confirm if it is their view that LPP applies to the solicitor's actions. The Director of Corporate Services reserves the right to seek external legal advice on the matter if they so wish. The Director of Corporate



Services should decide in a timely manner. If they determine LPP applies, then the MLRO/DMLRO will not report the matter to the NCA.

6.10 Where consent is required from the NCA for a transaction to proceed (and 6.8 does not apply), then the transactions in question must not be undertaken or completed 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.

6.11 The MLRO/DMLRO commits a criminal offence if he knows or suspects, or has reasonable grounds to do so, through a disclosure being made to him:

- That another person is engaged in money laundering of whom he knows the identity,
- The whereabouts of laundered property in consequence of the disclosure, that the person or property's whereabouts can be identified from that information,
- He believes, or it is reasonable to expect him to believe, that the information will or may assist in such identification and he does not disclose this as soon as practicable to the NCA (unless an exemption applies as per 6.8)

7. Customer due diligence

7.1 When the council is carrying out certain regulated business (accountancy, and legal services re financial, company or property transactions) and as part of this,

- a) Forms an ongoing business relationship with a client; or
- b) Undertakes a one-off or occasional transaction amounting to €15,000 or more whether carried out as a single transaction or several linked ones; or
- c) Suspects money laundering or terrorist financing; or
- d) Doubts the veracity or adequacy of information previously obtained for the purposes of client identification or verification.

7.2 Then the customer due diligence procedure must be followed before any business or transaction is undertaken for that client. This is covered in regulations 27-38 of the MLR 2017.

7.3 Customer due diligence means:

- Identifying the client/customer and verifying their identity based on documents, data, or information obtained from a reliable and independent source (e.g. conducting a search at companies house);



- Identifying the beneficial owner (where he/she or it is not the client) so that you are satisfied that you know who the beneficial owner is, including, in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangement; and
- Obtaining information on the purpose and intended nature of the business relationship.

7.4 Customer due diligence, including record keeping requirements, is set out in the following hyperlinks and relates to all customers:

- [Your responsibilities under money laundering supervision - GOV.UK \(www.gov.uk\)](https://www.gov.uk)
- [Quick guide to the Money Laundering Regulations 2017 | The Law Society](#)

Please note that unlike the reporting procedure, the customer due diligence procedure is restricted to those employees undertaking relevant business.

7.5 In the above circumstances, employees in the relevant services of the council must obtain satisfactory evidence of the identity of the prospective customer/client, and full details of the purpose and intended nature of the relationship/transaction, as soon as practicable after instructions are received.

7.6 There is also now an ongoing legal obligation to check the identity of existing clients and the nature and purpose of the business relationship with them at appropriate times. The opportunity should also be taken at times to scrutinise the transactions undertaken throughout the course of the relationship (including, where necessary, the source of the funds) to ensure they are consistent with your knowledge of the client, its business and risk profile. Particular scrutiny should be given to the following:

- a) complex or unusually large transactions;
- b) unusual patterns of transactions which have no apparent economic or visible lawful purpose; and
- c) any other activity likely by its nature to be related to money laundering or terrorist financing.

7.7 Once instructions to provide relevant business have been received, and it has been established that Paragraph 7.1 above applies or it is otherwise an appropriate time to apply due diligence measures to an existing client, evidence of identity and information about the nature of the work should be obtained/checked as follows.

8. Internal Clients

8.1 Under the legislation there is no need to apply customer due diligence (CDD) measures where the client is a UK public authority. So internal clients of Lancashire County Council do



not fall into the scope of these measures. If the client is not wholly owned by Lancashire County Council, the identity of the other party who has interests should continue to be checked.

- 8.2 Appropriate evidence of identity will be placed on the council's client file along with a prominent note explaining which correspondence constitutes the evidence and where it is located.
- 8.3 If there is any ambiguity around the need for CDD a decision can be made on a case-by-case basis by consulting with the DMLRO.

9. External clients

- 9.1 When the council provides regulated business services to another UK public authorities, there is no need to apply customer due diligence measures. However, again as a matter of good practice, identity of external clients should be checked.
- 9.2 Appropriate evidence of identity will be placed on the council's client file along with a prominent note explaining which correspondence constitutes the evidence and where it is located.
- 9.3 With instructions from new clients, or further instructions from a client not well known to you, you may wish to seek additional evidence of the identity of key individuals in the organisation and of the organisation itself.

10. Simplified due diligence

- 10.1 Simplified due diligence is the lowest level of due diligence that can be completed on a customer. This is appropriate where there is little opportunity or risk of your services or customer becoming involved in money laundering or terrorist financing.
- 10.2 Where a customer is low risk (occupation; organisation; country; method of transacting; transaction value etc.) then simplified due diligence can be completed. Identity must still be confirmed but the ongoing requirements may be relaxed unless a change in circumstances occurs.

11. Enhanced customer due diligence and ongoing monitoring

- 11.1 It will, in certain circumstances, be necessary to undertake what is known in the regulations as enhanced customer due diligence. In summary, this will be necessary where:
- The customer has not been physically present for identification purposes; or



- The customer is a politically exposed person, typically, a non UK or domestic member of parliament, head of state or government, or government minister and their family members and known close associates
- There is a beneficial owner who is not the customer – a beneficial owner is any individual who: holds more than 25% of the shares, voting rights or interest in a company, partnership or trust.
- When you enter into a transaction with a person from a high risk third country identified by the EU [Register of Commission Documents - C\(2016\)4180 \(europa.eu\)](https://eur-lex.europa.eu/eli/reg/2016/4180/oj)
- In any other situation which, by its nature, can present a higher risk of money laundering or terrorist funding.

11.2 Where this applies, the council will need to take adequate measures to compensate for the higher risk.

11.3 MLR 2019 prescribes what is required at a minimum. When enhanced due diligence is performed, it must always involve:

- a) Obtaining additional information on the customer and on the customer's beneficial owner
- b) Obtaining additional information on the intended nature of the business relationship
- c) Obtaining information on the source of funds and source of wealth of the customer and of the customer's beneficial owner
- d) Obtaining information on the reasons for the transactions
- e) Obtaining the approval of senior management for establishing or continuing the business relationship
- f) Conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination.

11.4 If, because of customer due diligence checks, there are any discrepancies identified when compared with the information held in the Companies House register, then this must be reported to Companies House.

12. Red flag indicators

12.1 Red flags is the term used to describe individual factors set by the council that indicates a higher risk of money laundering or terrorist financing. These should act as a warning that further investigation is necessary. **Appendix D** sets out examples of 'red flag indicators'



12.2 Red flags should be used at all stages of compliance, from customer acceptance to exiting the relationship. Red flags fall into different categories but are usually centred around client behaviours or issues around the Authority, its finance, beneficiaries or trading connections to high-risk individuals or jurisdictions.

13. Record keeping

13.1 Each area conducting relevant business must maintain records of:

- Client identification evidence obtained
- Details of all relevant business transactions carried out for clients

13.2 For at least five years. This is to meet the requirements of the MLR 2017 and may be used as evidence in any subsequent investigation/inspection by the relevant supervising body. Any record keeping should be in line with GDPR and the originating department's Privacy Statement.

13.3 In practice each area will be routinely making records of work carried out during normal business and these should suffice in this regard.

13.4 Each area of the council conducting regulated business must monitor, on an ongoing basis, their business relationships in terms of scrutinising transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with their knowledge of the client, its business and risk profile.

13.5 Individuals carrying out due diligence checks must retain the identification evidence and details of the relevant transaction(s) for that client for at least five years.

13.6 The DMLRO will keep a record of all referrals received and any action taken to ensure an audit trail is maintained.

14. Training and staff awareness

14.1 The council will take appropriate measures to ensure that all employees are made aware of the law relating to money laundering and will arrange targeted, ongoing training to key individuals most likely to be affected by the legislation.

14.2 It is extremely important that all employees are familiar with their legal responsibilities: serious criminal sanctions may be imposed for breaches of the legislation. The key requirement on employees is to promptly report any suspected money laundering activity to the DMLRO.



15. Risk management and internal control

- 15.1 The legislative requirements concerning anti-money laundering procedures are lengthy and complex. The adequacy and effectiveness of, promotion of, and compliance by employees with, the documentation and procedures will also be monitored through the county council’s corporate governance and anti-fraud policy frameworks.
- 15.2 This policy has been written so as to enable the council to meet the legal requirements in a way which is proportionate to the risk of the council of contravening the legislation.
- 15.3 The MLRO and the DMLRO will periodically review the risk to the county council of contravening the anti-money laundering legislation. The adequacy and effectiveness of the anti-money laundering policy will be reviewed after such assessments.
- 15.4 Should you have any concerns generally or about specific transactions then you should contact the MLRO or the DMLRO.

16. Version Control

Named Owner:	P Walker, Senior Investigator, Internal Audit
Version Number:	1.0
Date Of Creation:	November 2021
Last Review:	September 2022
Next Scheduled Review:	September 2023
Overview of Amendments to this Version:	



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 and an unlimited fine. At the Magistrates Court it is 6 months and £5,000 fine
S328 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 were stolen goods is not guilty. The punishment is as per 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 per 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



		<p>in money laundering and does not make a report through the appropriate channels.</p> <p>Negligence is not a defence as the employee will be tried upon what they should have known given their experience, knowledge and training.</p> <p>This is punishable by a maximum term of imprisonment of 5 years and/or a fine.</p>
S331 Proceeds of Crime Act 2002	Failure to Disclose Offence: Nominated Officers in the Regulated Sector	<p>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.</p> <p>Negligence is not a defence as the nominated officer will be tried upon what they should have known given their experience, knowledge and training.</p> <p>This is punishable by a maximum term of imprisonment of 5 years and/or a fine.</p>
S332 Proceeds of Crime Act 2002	Failure to Disclose Offence: Other Nominated Officers	<p>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.</p> <p>This is punishable by a maximum term of imprisonment of 5 years and/or a fine.</p>
S333 Proceeds of Crime Act 2002	Tipping Off Offence	<p>This offence is committed if an employee or Member makes a disclosure which is likely to prejudice an investigation</p>



		<p>being carried out by a law enforcing authority, knowing that such an investigation is in motion.</p> <p>This is punishable by a maximum term of imprisonment of 5 years and/or a fine.</p>
<p>Reg 86 Money laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017</p>	<p>Contravening a relevant requirement</p>	<p>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.</p> <p>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.</p>
<p>Reg 87 Money laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017</p>	<p>Prejudicing an investigation</p>	<p>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.</p> <p>The punishment is as for Reg. 86 above</p>
<p>Reg 88 Money laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017</p>	<p>Providing false or misleading information</p>	<p>There are two separate offences under regulation 88.</p> <p>Under regulation 88(1) a person commits an offence if:</p> <ol style="list-style-type: none"> 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



		<p>2. Is reckless as to whether the information is false or misleading. In respect of both offences.</p> <p>The punishment is the same as Regs 86 and 87 above</p>
--	--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------



Appendix B

Possible signs of money laundering:

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 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 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).
- 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 or 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 DMLRO.

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.



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 shouldn't be reported.

ACTIVITY	The types of activity that may be affected
New customers with high value transactions	<ul style="list-style-type: none"> - Selling property to individuals or businesses - Renting out property to individuals or businesses - Entering into other lease agreements - Undertaking services for other organisations
Secretive clients	<ul style="list-style-type: none"> - 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 funding was used for
Customers who we think are acting dishonestly or illegally	<ul style="list-style-type: none"> - People paying for council services who do not provide details about themselves - People making odd or unusual requests for payment arrangements Illogical transactions <ul style="list-style-type: none"> • 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 - Payments of substantial sums by cash - Large debt arrears paid in cash - Refunding overpayments - Deposits / payments for property
Payments of substantial sums by cash	Large debt arrears paid in cash <ul style="list-style-type: none"> - Refunding overpayments - Deposits / payments for property
Movement of funds overseas	Requests to pay monies overseas, potentially for "tax purposes"
Cancellation of earlier transactions	<ul style="list-style-type: none"> - 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



<p>Requests for client account details outside normal course of business</p>	<ul style="list-style-type: none"> - Queries from other companies regarding legitimacy of customers - council receiving correspondence /information on behalf of other companies
<p>Extensive and overcomplicated client business structures /arrangements</p>	<ul style="list-style-type: none"> - Requests to pay third parties in respect of goods / services - Receipt of business payments (rent,) in settlement from seemingly unconnected third parties
<p>Poor accounting records and internal financial control</p>	<ul style="list-style-type: none"> - Requests for grant funding / business support indicates third party 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
<p>Unusual property investment or transactions</p>	<ul style="list-style-type: none"> - Requests to purchase council assets / land with no apparent purpose - Requests to rent council property with no apparent business motive
<p>Overcomplicated legal arrangements / multiple solicitors</p>	<p>Property transactions where the council is dealing with several different parties</p>



Appendix C

Red Flag Indicators of potential money laundering

Red flag indicators **should always** prompt you to raise questions in your mind and these should prompt you to make further enquiries. Please note this is not an exhaustive list.

The answers (or failure to answer) will either dispel the original suspicion that something may not be quite right or reinforce that suspicion or highlight new areas for investigation.

Customer / Client Behaviour

When risk assessing a client, there are some red flag behaviours that should raise questions in your mind and cause you to make further enquiry. These include:

- avoiding personal contact without good reason.
- changing agent or legal advisor a number of times without apparent reason.
- using an advisor geographically distant from himself or the location of the transaction over using an advisor closer to the transaction.
- requesting or seeking to push the speed of the transaction.
- attempting to disguise the true owner or proprietary interests of the business or the parties to the transaction.
- the client is known to have convictions for acquisitive crime or criminal connections.
- the client informs you that funds are coming from one source and then at the last minute the source changes.

Source or Amount of Finance

The source of finance does not make sense, including:

- use of disproportionate amount of cash.
- funds sent to and from jurisdictions with a high level of banking secrecy.
- a significant amount of private funding from an individual running a cash-intensive business.
- the involvement of a third party without an apparent connection to the business or without a full explanation for their participation.
- funding which is inconsistent with the socio-economic profile of the individuals involved.
- a 100% cash deal.
- structured payments below money laundering thresholds.



The Business

Red flags include:

- the ownership structure is overly complicated when there is no legitimate or economic reason.
- business transactions involve countries where there is a high risk of money laundering and / or the funding of terrorism.
- false or suspicious documents are used to back-up transactions.
- the level of activity is not consistent with the firm's understanding of the client's business or level of legitimate income.
- a failure to produce adequate paperwork detailing the business and its formation.
- a history of aborted transactions.
- unverifiable information produced.



APPENDIX D – Proforma Disclosure Report

CONFIDENTIAL: Report to Money laundering Reporting Officer	
Name	
Title / Department / Directorate	
Phone number	
Email	
Details of Suspected Offence	
Names and addresses of the persons involved (if a company, the nature of their business)	
Nature, value, timing of activity	
Nature of suspicions	
Signed and dated (type name and date)	
For Completion by the DMLRO	
Date received	
Are there reasonable grounds for suspecting money laundering?	
If yes, confirm date of report to NCA	
Unique NCA case reference number	
Date consent given to employee for transaction to proceed (if applicable)	
Signed and dated	
<p>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.</p>	



