Anti-Money Laundering Policy

Document Owner	Zena Cooke Corporate Director of Finance
Version	Version 7

Version	Reviewed	Reviewer	Approver	Date approved
Original				
2	29 Sept 2014	Internal Audit	Governance & Audit Committee	29 Jan 2015
3	16 Oct. 2017	Internal Audit	Governance & Audit Committee	1 Nov 2017
4	05 Sept 2018	Internal Audit	Governance & Audit Committee	24 Oct 2018
5	06 Sept 2019	Internal Audit	Governance & Audit Committee	21 Jul 2020
6	14 Dec 2021	Internal Audit	Governance & Audit Committee	25 Jan 2022
7	07 Feb 2024	Internal Audit	Governance & Audit Committee	TBC

1. Introduction

1.1. Kent County Council has a zero tolerance policy concerning money laundering and is committed to the highest standards of conduct.

1.2. The Proceeds of Crime Act (POCA) 2003, the Terrorism Act 2000 and the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 place obligations on Kent County Council and its employees to ensure that procedures are in place to prevent the Council's services being used for money laundering.

1.3. This policy sets out the process to minimise the risk, as well as provide guidance on the Council's money laundering procedures. Adhering to this policy and guidance will protect employees from the risk of prosecution if an employee becomes aware of money laundering activity while employed by the Council.

1.4. The policy is not intended to prevent customers and service providers from making payments for Council services, but to minimise the risk of money laundering in high value cash transactions.

2. Policy Statement

2.1. Kent County Council is committed to:

- Preventing the Council's services and employees from becoming a victim of, or unintentional accomplice to, money laundering activities.
- Identifying the potential areas where money laundering may occur and strengthening procedures to minimise the risks.
- Complying with all legal and regulatory requirements, with particular regard to the reporting of actual or suspected cases of money laundering.

2.2. It is important that every member of staff is aware of their responsibilities and remains vigilant.

3. Scope of Policy

3.1. This policy applies to **all** employees and Members of the Council, whether permanent or temporary.

3.2. The aim of this policy is to support employees and Members in responding to financial concerns that have been highlighted in the course of their work for the Council. If staff or Members are concerned about a financial matter unrelated to work, the Police should be contacted.

4. Definition of Money Laundering

4.1. The term ‘Money Laundering’ can be used to describe a number of offences involving the proceeds of crime or terrorist financing. In simple terms, money laundering is a process used by criminals to make the proceeds of their crimes appear as though they originated from a legitimate source. Money launderers aim to disguise the identity of the criminal and/or conceal their connection to the proceeds of the crimes.

4.2. The following constitute money laundering offences:

a) Concealing, disguising, converting, transferring criminal property or removing it from the UK (s327 of the POCA 2002).

b) 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 (s328 of the POCA 2002).

c) Acquiring, using or possessing criminal property (s329 of the POCA 2002).

d) Doing something that might prejudice an investigation e.g. falsifying a document (s333 of the POCA).

e) Failure to disclose one of the offences listed in a) to c) above, where there are reasonable grounds for knowledge or suspicion (s330-332 of the POCA 2002).

f) Tipping off a person(s) who is or is suspected of being involved in money laundering in such a way as to reduce the likelihood of or prejudice an investigation (s330 of the POCA 2002).

4.3. There is a possibility that any member of staff could be prosecuted for money laundering offences if they suspect money laundering and either become involved with it in some way and/or do nothing about it. This policy sets out the appropriate practice and how any concerns should be raised.

4.4. Although the risk to the Council of contravening the legislation is low, it is important that all employees are aware of their responsibilities as serious criminal sanctions may be applied to those who breach the legislation.

4.5. **The significant requirement for employees is to immediately report any suspected money laundering activity to the Money Laundering Reporting Officer (MLRO; see section 7.1). Failure to do so could lead to prosecution.**

5. Identifying Money Laundering

5.1. There is no clear definition of what constitutes a suspicion of money laundering – common sense will be needed, see Annex 1 for a list of areas that may be affected. Although there does not need to be actual evidence that money laundering is taking place, mere speculation is unlikely to be sufficient to give rise to knowledge or suspicion. However, if you deliberately shut your mind to the obvious, this will not absolve you of your responsibilities under the legislation.

5.2. Examples of money laundering activity include:

- Large cash payments;
- Asking for cash refunds on credit card payments; or
- Overpaying bills and invoices and then asking for cash refunds.

5.3. Any transaction involving an unusually large amount of cash should cause concern and prompt questions to be asked about the source. This will particularly be the case where the value of cash paid exceeds the amount due to settle the transaction and the person(s) concerned ask for a non-cash refund of the excess.

5.4. If the person(s) concerned use trusts or offshore funds for handling the proceeds or settlement of a transaction, then the reasons for this should be questioned.

5.5. Care should be exercised and questions asked where:

- A third party intermediary becomes involved in a transaction;
- The identity of a party is difficult to establish, or is undisclosed;
- A company is used where the ultimate ownership of the company is concealed or difficult to verify; and/or
- A party is evasive about the source or destiny of funds.

6. The Council's Obligations

6.1. The Council is obligated to:

- Appoint a money laundering reporting officer;
- Maintain client identification procedures in certain circumstances;
- Implement a procedure to enable the reporting of suspicions of money laundering;

- Report any cash transactions over €10,000 (or the Sterling equivalent);
- Provide training to officers at risk of being exposed to money laundering;
- Maintain sufficient records.

7. The Money Laundering Reporting Officer (MLRO)

7.1. The Council has nominated the following officers to be responsible for anti-money laundering measures within the Council:

MLRO: Corporate Director of Finance

Deputy MLRO: Head of Internal Audit & Counter Fraud

7.2. In the absence of the MLRO or in instances where it is suspected that the MLRO themselves are involved in suspicious transactions, concerns should be raised with the Chief Executive Officer.

8. Further information

8.1. Further information can be obtained from the MLRO and the following websites:

- www.nationalcrimeagency.gov.uk
- Proceeds of Crime (Anti- Money Laundering) - Practical Guidance for Public Service Organisations'- CIPFA
- Money Laundering Guidance at www.lawsociety.org.uk
- HM Revenue & Customs http://www.hmrc.gov.uk/mlr/

9. Conclusion and Risk Assessment

9.1. The risk of Kent County Council service being exposed to money laundering is extremely low. This is assessed due to the low amount of cash Kent County Council receives that are from known cash income sources and low volumes and low amounts of refunds being made. However, the legislation and requirements that have been implemented must be followed. Failure to comply with such legislation and requirements by individuals could lead to prosecution.

Anti Money Laundering Procedures

1. Reporting concerns

1.1. In the event of an employee suspecting a money laundering activity they must immediately report their suspicion to the MLRO, or to the deputy MLRO, using the disclosure report available on Knet. The report must contain as much detail as possible, ideally using the form at Annex 2.

1.2. If the suspicious transaction is happening right now, for example someone is trying to make a large cash payment, every effort should be made to speak with the MLRO or deputy, who will decide whether to accept the payment or suspend the transaction. If it is not practical or safe to do so, a report should be made to the MLRO or deputy immediately after the transaction is complete.

1.3. The information provided to the MLRO will be used to decide whether there are reasonable grounds to demonstrate knowledge or suspicion of money laundering, whether further investigation is necessary, whether the transaction should be accepted or suspended, and if appropriate, whether a suspicious activity report should be made to the National Crime Agency (NCA). If it is not practical or safe to suspend a suspicious transaction a report should be made to the National Crime Agency immediately after the transaction is complete.

1.4. The employee must follow directions given to them by the MLRO and must **not** discuss the matter with others or notify the person(s) who is suspected of money laundering. 'Tipping off' a person suspected of money laundering is a criminal offence.

1.5. The MLRO or deputy must immediately evaluate any disclosure to determine whether the activity should be reported to the National Crime Agency (NCA).

1.6. The MLRO or deputy must, if they so determine, promptly report the matter to NCA in a prescribed manner and on their standard report form (currently referred to as a suspicious activity report (SAR)). This can be found on the NCA website: www.nationalcrimeagency.gov.uk

2. Identification of Clients

2.1. In general, management should ensure that appropriate checks are carried out on new partners, suppliers and contractors in accordance with the Council's existing policies and procedures.

2.2. However, where the Council is carrying out a **'relevant business**',[1] and as part of this:

- forms an ongoing business relationship with a client; or
- undertakes a one-off transaction involving payment by or to the client of €10,000 (or the equivalent in sterling) or more; or
- cash payments totalling €10,000 or more which appear to have been broken down into smaller amounts so that they come below the high value limit; or
- it is known or suspected that a one-off transaction (or a series of them) involves money laundering.

2.3. Then the client identification procedures (listed below) must be followed before any business is undertaken for that client.

2.4. Where the 'relevant business' is being provided internally signed, written instructions on Council headed notepaper or an email on the internal email system should be provided at the outset of the business relationship.

2.5. If the 'relevant business' is being provided externally then the following additional checks must be completed:

- Check the organisation's website and other publicly available information such as telephone directory services and Companies House to confirm the identity of the personnel, their business address and any other details;
- Ask the key contact officer to provide evidence of personal identity and position within the organisation, for example a passport, photo ID card, driving licence and signed, written confirmation from the Head of Service or Chair of the relevant organisation that the person works for the organisation. This can be obtained through electronic ID verification if it is free from fraud and provide sufficient assurance of the identity of the individual;
- Enhanced due diligence will be required for any transaction where the organisation is established in a high-risk third country, or where the transaction is complex or unusually large.

2.6. Remember, these additional client identification procedures are **only** required when conducting a 'relevant business.'

3. The types of activities that may be affected

3.1. The following table sets out the types of activities that might be suspicious, and how the Council may come across those activities. It is not intended to be

[1] Relevant business is defined as the provision 'by way of business' of advice about tax affairs; accounting services; audit services; legal services; services involving the formation, operation or arrangement of a company or trust; or dealing in goods wherever a transaction involves a cash payment of €10,000 or more

exhaustive, and just because something you are suspicious about is not on the list, it doesn't mean you shouldn't report it.

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 other lease agreements • Undertaking services for other organisations
Secretive clients	• 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	• 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 in foreign currencies for no apparent reasons
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 good / service has been provided • Sudden and unexpected termination of lease agreements
Requests 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 overcomplicated client business structures /	• Requests to pay third parties in respect of goods / services • Receipt of business payments (rent, business rates) in settlement from seemingly unconnected third parties

arrangements	
Poor accounting records and internal financial control	• 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
Unusual property investments 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

4. Training

4.1. Officers considered to be most at risk of being exposed to suspicious situations will be made aware by their senior officer and provided with appropriate training.

4.2. Additionally, all officers and Members will be familiarised with the legislation and regulations relation to money laundering and how they affect the employees (themselves) and the Council.

4.3. It is not necessary for all staff to be aware of the specific criminal offences, staff that are likely to encounter money laundering should be aware of the procedures that are in place. This policy and procedures provides sufficient information to raise awareness for most staff.

4.4. It is recommended that staff in areas that are highly vulnerable to money laundering, should be provided with targeted training that is specific to the Council activity at hand. This could be achieved by in-house resources, or through training courses and seminars run by external provider.

Annex 2

Anti Money Laundering Reporting Form

Your Contact Details

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

Name :	
Role:	
Email:	
Contact Telephone:	

Main Subject

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

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

Transaction(s)

Please enter the details of the transactions you think are suspicious

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

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

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

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

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

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

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

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

Linked addresses:
Please enter details of any linked addresses:

Address	Type: (Home, work etc)	

Reason for Suspicion:
Please enter details of your suspicions. Please provide as much information as possible.
