

Anti-Money Laundering Policy

Overview

‘Money laundering’ is something criminals do to hide the cash they make from crime. This money may come from any criminal activity. This could include terrorism, drugs trafficking, corruption, tax evasion and theft. Money laundering tries to make this money look like it has a legitimate origin. This is usually done by passing the money through different organisations.

Any organisation which processes large volumes of financial transactions could, in theory, be used by criminals to launder money. Additionally, some Council service users may be vulnerable to being targeted by individuals seeking to use them as part of money laundering networks.

The aims of this policy are to:

- Help staff understand what money laundering is and how to recognise the warning signs.
- Require everyone to report suspicions about money laundering or terrorist financing. Reports should be made to the Head of Internal Audit & Risk Management (see Section 5).
- Explain Cambridgeshire County Council’s approach to identifying and reducing the risk of money laundering. Demonstrate how this aligns with best practice.
- Safeguard the Council and its service users from the risk of involvement in money laundering or terrorist financing networks.

This policy applies to all employees (including agency staff), staff at maintained schools, contractors, Members and agents of the Council. The Council expects all its employees, members and associated persons to act legally, with integrity, and in accordance with the Council’s values and policies at all times.

Policy Owner
Name: Mairead Claydon
Post: Acting Head of Internal Audit & Risk Management
Email: Mairead.Claydon@cambridgeshire.gov.uk

Anti-Money Laundering Policy

Table of Contents:

- 1. Introduction**
- 2. What is money laundering?**
 - 2.1 Understanding 'money laundering'
 - 2.2 How does money laundering affect the Council?
- 3. What are the warning signs of money laundering?**
 - 3.1 Warning signs for possible money laundering
 - 3.2 Council activities which are more high-risk for money laundering
- 4. What steps does Cambridgeshire County Council take to address potential money laundering?**
 - 4.1 Money Laundering Reporting Officer
 - 4.2 Internal Procedures
 - 4.3 Guidance & Training for Key Staff
- 5. How can you report any concerns about money laundering?**
 - 5.1 How to report concerns
 - 5.2 What happens after you report possible money laundering?
- 6. Customer Due Dilligence**
 - 6.1 What is Customer Due Diligence?
 - 6.2 When must the Customer Due Diligence process be followed?
- 7. How is this policy reviewed and monitored?**

Appendices:

- 1 Overview of Money Laundering Offences**

Anti-Money Laundering Policy

1. Introduction

- 1.1 This Anti-Money Laundering Policy shows how Cambridgeshire County Council seeks to reduce the risk of money laundering in Council systems .
- 1.2 The Council recognises that most people are honest and would never intentionally allow money laundering to take place using Council systems. This policy provides a safeguard against the risk of money laundering as well as guiding staff, Members and service users on how to identify and report possible money laundering activity.
- 1.3 This policy applies to all employees (including agency staff), contractors, Members and agents of the Council. It is part of the Council's anti-fraud policy framework.

2 What is money laundering?

2.1 Understanding 'money laundering'

- 2.1.1 'Money Laundering' is something criminals do to hide the cash they make from crimes or political corruption. Usually this involves making lots of different financial transactions with the cash. This makes it difficult for the police to find out where the criminal got the money. The criminals can then deposit the money into a bank account and use the money without suspicion.
- 2.1.2 There are lots of different ways that criminals can try to hide the origins of their money. For example:
 - Criminals put fake transactions into the books of a business which receives a lot of cash payments (such as a takeaway or launderette). Then the cash they have made from crime can be treated as proceeds of the business.
 - Criminals pass the money through a third party bank account or business. This makes it difficult for anyone to see where the money originally came from.
 - Criminals buy property or assets using cash, then sell it. The money they get from this will then be treated as legitimate proceeds from the sale.

2.2 How does money laundering affect the Council?

- 2.2.1 This might not sound like something that is likely to affect Cambridgeshire County Council. However, there are several specific criminal offences relating to money

laundering which may apply to public authorities and their staff, including Cambridgeshire County Council. Full details of these offences are set out in Appendix 1, below.

- 2.2.2 Anyone who has enabled a transaction linked to money laundering could be held liable and charged with money laundering offences. This could affect Council officers who are making financial transactions as part of their job.
- 2.2.3 However, if you report any suspicions about money laundering, you won't be charged with a crime. That's why it's important for Council employees to be aware of the warning signs of possible money-laundering, and to know how to report any concerns. See Section 3.2 for some areas of the Council that may be at higher-risk for money laundering

3 What are the warning signs of money laundering?

- 3.0.1 Money laundering is so complicated that it isn't possible to give a complete list of ways to identify money laundering. We've set out some risk factors which may suggest possible money laundering activity, and areas within the Council that are more high-risk.
- 3.0.2 Remember: if you're not sure, you can always contact Internal Audit at internal.audit@cambridgeshire.gov.uk for further advice.

3.2 Warning signs for possible money laundering:

- 3.1.1 The below warning signs could be an indication of possible money laundering:
- If an individual or a business wants to make a large payment in cash, and/or insists on paying in cash when this isn't normal.
 - If an individual or business over-pays the Council and then asks for the money to be 'paid back'. This is especially concerning if they request repayment by cheque or to a different bank account.
 - Where a third party is involved in a transaction for no obvious reason. For instance, if the Council is purchasing an item from Company A, but it is requested that payment is made to Company B.
 - Unusual transactions or ways of conducting business, without reasonable explanation.
- 3.1.2 Council officers should also be mindful that vulnerable individuals may be targeted by criminals as a way of laundering money. Individuals may think they have a 'job'

handling 'money transfers'. Or they may be asked to receive a money transfer (often from abroad) and then withdraw it in cash, as a favour for a friend. If you suspect that a vulnerable individual is being targeted in this way, please report it. Even if there is no financial impact on the Council's funds, it may be a safeguarding issue.

3.2 Council activities which are more high-risk for money laundering:

3.2.1 In theory, money laundering could take place wherever money is moving in and out of the organisation. However, there are some activities that are more high-risk than others.

3.2.2 Many of these activities are likely to involve third party suppliers (such as banks, estate agents or solicitors). These organisations should have their own anti-money laundering arrangements in place. Equally, it is important not to rely on external organisations to identify possible issues. You should always report any concerns you have about money laundering, even if you think that they're likely to be identified elsewhere.

3.2.3 The areas of Council activity that have been identified as being higher risk for money laundering are:

- **Cash transactions:** Cash transactions (including notes, coins and travellers cheques) are higher risk for money laundering. The Council has a policy not to accept cash payments above £7,500. However, large or unusual cash payments below this amount may still be suspicious. All such payments should be reported to the Council's Money Laundering Reporting Officer (see Section 4.1).
- **Sales and purchases of property:** Purchasing and selling property is popular with money launderers. Property sales provide an opportunity to launder a large sum of money in a single transaction. Solicitors handling property transactions are legally required to undertake money laundering checks. Staff involved in property transactions should still be aware of possible warning signs for money laundering and know how to report concerns. Warning signs of possible money laundering when purchasing or selling property include:
 - Transactions taking place in cash, especially if the price seems unusually low (or high).
 - Transactions taking place via an intermediary.
 - Transactions on behalf of minors, trusts, or individuals without capacity.

- Transactions with anyone who seems to lack the financial means to make the purchase or own the property.
- Properties which are owned by overseas individuals or companies.
- Transactions for the same property that happen in quick succession. For example: a purchase, then immediate sale. This is especially a risk if there is a large change in price.
- Purchases made from 'off market' agents who are not required by law to be registered for money laundering supervision. This includes house builders and some construction companies.
- **Direct Payments and Prepaid Cards:** Service users who have a Direct Payments bank account and/or a reloadable prepaid card they can use to spend their direct payment or other money may be targeted by criminals seeking to use these accounts to launder money via 'money muling'. Money muling occurs when an individual receives money into their bank account and transfers it elsewhere or withdraws it as cash. The individual is often promised that they can keep some of the cash. They may not be aware that the money is criminal in origin. Warning signs of this type of activity in Direct Payment accounts or prepaid cards include:
 - Money going into the account and then quickly being transferred or withdrawn, especially if the amounts are significant.
 - A third party loading money onto the card or transferring into the account.

4. What steps does Cambridgeshire County Council take to address the risk of money laundering?

4.0.1 Public sector organisations are not regulated by the Money Laundering Regulations. However, CIPFA recommends that local authorities operate in the spirit of these regulations. CIPFA's guidance on Combating Financial Crime states that all public authorities that have not already done so need to use a risk-based approach in deciding the extent to which their activities are exposed to the dangers of money laundering, and to take proportionate steps to address these dangers.

4.0.2 As a minimum, CIPFA recommends public authorities should:

- Arrange for a nominated officer to receive, review and pass on any concerns about suspicious activity or possible money-laundering (see Section 4.1).

- Establish proportionate and cost-effective internal procedures to prevent and detect money laundering and terrorist financing (see Section 4.2).
- Identify staff most likely to encounter money laundering or terrorist financing and:
 - Ensure they are aware of any requirements and obligations placed on the authority, its staff, and on them as individuals, by the Proceeds of Crime Act (POCA) and the Terrorism Act (TACT);
 - Give targeted training to these staff (see Section 4.3).

4.0.3 This section shows how the Council has ensured it is compliant with these recommendations.

4.1 Money Laundering Reporting Officer:

4.1.1 CIPFA recommend that public authorities appoint a Money Laundering Reporting Officer (MLRO). The MLRO is responsible for receiving internal reports about possible money laundering. They then report any suspicious money laundering activities to the National Crime Agency.

4.1.2 At Cambridgeshire County Council, the Head of Internal Audit & Risk Management is the MLRO. In the absence of the MLRO, the Monitoring Officer stands in as the Deputy MLRO.

Money Laundering Reporting Officer	Deputy Money Laundering Reporting Officer
Mairead Claydon, Acting Head of Internal Audit & Risk Management	Fiona McMillan, CCC Director of Legal and Governance (Monitoring Officer)
Email address: mairead.claydon@cambridgeshire.gov.uk	Email address: Fiona.mcmillan@cambridgeshire.gov.uk
Phone: 01223 715542	Phone: 01733 452409

4.1.3 The procedure for reporting to the Money Laundering Reporting Officer is in Section 5, below. You can report any form of suspicious financial activity to the MLRO. Staff must get in touch with the MLRO whenever they have reasonable grounds to suspect money laundering may be taking place, or has taken place.

4.1.4 The MLRO will keep a record of all referrals received. They will also record any action taken to report concerns on to the National Crime Agency.

4.1.5 The MLRO also has ownership of this Anti-Money Laundering Policy. They also own the Council's money laundering and terrorist financing risk assessment. The MLRO supports and co-ordinates the response to money laundering risk across the organisation.

4.2 Internal Procedures:

- 4.2.1 This Anti-Money Laundering Policy is part of a wider anti-fraud framework at Cambridgeshire County Council. This includes our Whistleblowing Policy and Anti-Fraud & Corruption Policy.
- 4.2.2 As part of the development of this policy, the Council has conducted a risk assessment. This looks at money laundering and terrorist financing risks across different service areas. It confirms the key corporate controls in place to prevent money laundering. It also identifies any further actions to be undertaken by the Council to further reduce these risks. The risk assessment and policy are reviewed regularly.
- 4.2.3 Cambridgeshire County Council has implemented a reporting procedure (see Section 5 for more details). This enables staff with any concerns about money laundering to report them.
- 4.2.4 Cash payments do not represent a large proportion of the Council's financial transactions. However, they do represent a higher risk for money laundering and terrorist financing. To reduce this risk, the Scheme of Financial Management confirms that the Council will not accept cash payments above £7,500. Only the Chief Finance Officer may approve higher cash payments, in exceptional circumstances. Officers are required to report any large and/or unusual cash transactions to the MLRO. This ensures any such transactions are subject to appropriate scrutiny.
- 4.2.5 Cambridgeshire County Council has implemented customer due diligence procedures (see Section 6). This is in line with CIPFA best practice. It aims to verify the identity of the people and organisations CCC trades with, in situations that are more high-risk for money laundering.
- 4.2.6 The Council's Treasury Management function has its own due diligence processes. The Council will only lend money or invest with counterparties who meet certain requirements. Treasury Management activities are subject to CIPFA's Code of Practice. For more information, see the Council's Treasury Management Strategy.

4.3 Guidance & Training for Key Staff:

- 4.3.1 This Anti-Money Laundering Policy provides guidance for all Cambridgeshire County Council staff. It explains how to identify possible money laundering concerns and report them.

- 4.3.2 The Money Laundering Reporting Officer runs annual awareness-raising campaigns. This includes work to raise awareness of this policy among all staff. Targeted communications are shared with staff in teams which may be higher-risk for money laundering.
- 4.3.3 Counter fraud e-learning, which covers money laundering risks, is available to all staff. Additionally, the Council periodically provides targeted money laundering training. This is focused on members of staff in key services which are more likely to be exposed to the risk of money laundering.

5. How can you report concerns about money laundering?

- 5.0.1 This section explains what you must do where you have any concern about money laundering or suspicious transactions, and how your report will be dealt with by the Money Laundering Reporting Office (MLRO).

5.1 How to report concerns:

- 5.1.1 If you have any concerns or suspicions about possible money laundering, terrorist financing or suspicious financial activity, it's really important to report them immediately – even if you think someone else may already have made a report. Please email the MLRO at mairead.claydon@cambridgeshire.gov.uk. Alternatively you can call or ask for a Teams meeting to discuss your concerns if you prefer this to emailing. If possible, it's helpful to provide the following information:
- The value and timing of the suspicious transaction(s) and what these related to.
 - Names and addresses of the people or companies involved.
 - Why you are suspicious of the transactions or activity.
- 5.1.2 It's really important if you suspect money laundering not to try to investigate the matter yourself. Don't tell anyone else about your suspicions, or the fact that you've made a report.
- 5.1.3 If you are suspicious about a particular transaction that is taking place, please do not proceed with or complete the transaction. For example, if you are concerned about an attempted cash payment, do not bank the cash. Or if you are concerned about a property purchase or sale, do not complete the purchase/sale. You must wait to complete the transaction until this is agreed by the MLRO in writing.

- 5.1.4 If you fail to report a suspicious transaction as soon as possible, this could be regarded as misconduct or gross misconduct by the Council. It could even amount to a criminal offence.

5.2 What happens after you report possible money laundering?

- 5.2.1 Once you've made a report to the MLRO, they will confirm to you that they have received the report and advise you when you will hear back from them. They will conduct an initial investigation into the matter. They may seek specialist advice if appropriate, depending on the circumstances.
- 5.2.2 The MLRO will then decide either:
- a) There are no reasonable grounds to suspect money laundering or terrorist financing. The MLRO will record the reasons for this finding and will agree for the transaction to proceed.
 - b) There are grounds to suspect money laundering. The MLRO will make a report to the National Crime Agency (NCA) and seek the NCA's consent for whether the Council can proceed with the transaction.
- 5.2.3 The MLRO will let you know their decision and what the next steps will be. They will also tell you about any consent or refusal from the NCA regarding whether the Council can proceed with the transaction.

6. Customer Due Dilligence

6.1 What is Customer Due Diligence?

- 6.1.1 'Customer Due Diligence' is a process the Council undertakes to reduce the risk of money laundering. The process aims to ensure that the Council only deals with real, legitimate organisations and customers.
- 6.1.2 When undertaking any financial transaction with an external organisation or individual, officers are responsible for ensuring that the person or organisation they are dealing with is legitimate. You should know who the 'ultimate beneficial owner' of the organisation is. This means the person or people who own and control the company.

6.1.3 Best practice is for this to involve verifying identity against a reliable and independent source. This should be done before any transaction takes place. For example, this could involve:

- **For companies:** Reviewing the company's website. Checking they are registered at Companies House. Obtaining a copy of their list of active directors and the statement of persons with significant control. Confirming this information aligns with what you know about the company.
- **For charities:** checking how they are registered (e.g. with the Charities Commission). Obtaining equivalent documentation.
- **For individuals:** viewing proof of identification.

6.1.4 If you can't verify the customer's identity, contact the Money Laundering Reporting Officer (see Section 5). If the results of the checks suggest that there may be a risk of money laundering, contact the Money Laundering Reporting Officer.

6.1.5 If the intention is that the person or organisation will be acting on behalf of the Council as part of this business relationship, you should consider how the Council's expectations around ethical conduct have been or will be communicated to them. Contractors must be aware that the Council will not tolerate fraud, bribery, money laundering or corruption. If you believe there may be a risk of unethical conduct or bribery by any person who will be acting on the Council's behalf, please consult the Monitoring Officer for advice. This must be done before establishing a business relationship.

6.2 When must the Customer Due Diligence process be followed?

6.2.1 In certain circumstances staff are obliged to undertake and formally record the Customer Due Diligence procedure. This includes:

- If the Council is carrying out regulated business (i.e. providing any accountancy, audit and tax services or legal services in respect of company, financial or property matters) for anyone other than another UK public authority and as a part of this:
 - Forms a new, ongoing business relationship with a client; and/or
 - Undertakes a one-off or occasional transaction equivalent to €15,000 or more (c. £12,500 at time of writing). This counts whether carried out as a single transaction or several linked ones.

- If the Council is carrying out transactions relating to cultural artefacts or items with archaeological, historical, cultural or religious significance, or rare scientific value.
 - If the Council doubts the veracity or legitimacy of any documents, data or information previously obtained for identification purposes.
 - If the Council suspects money laundering or terrorist financing.
- 6.2.2 When any of the above situations apply, details of the Customer Due Diligence check carried out must be recorded. Officers must also record details of the purpose and intended nature of the proposed business relationship.
- 6.2.3 Evidence of the checks undertaken should be retained for at least five years. If the business relationship continues, officers must ensure that the due diligence checks are repeated periodically.

7. How is this policy reviewed and monitored?

- 7.1 CCC Internal Audit is responsible for oversight and maintenance of this Anti-Money Laundering Policy. The Strategy & Resources Committee is the body responsible for approving any changes made to the policy, while the Audit & Accounts Committee is responsible for monitoring the policy.
- 7.2 If you require any additional guidance or support around this policy please contact either the MLRO or a member of the Internal Audit team at CCC through this email: internal.audit@cambridgeshire.gov.uk
- 7.2 Additionally, below are some useful links on the topic of money laundering:
- National Crime Agency <http://www.nationalcrimeagency.gov.uk>
 - The Law Society - Anti-Money Laundering Guidance and Advice - <http://www.lawsociety.org.uk/advice/anti-money-laundering>
 - Crown Prosecution Service definition of offences: [Money Laundering Offences | The Crown Prosecution Service \(cps.gov.uk\)](#)

Appendix 1

Overview of Money Laundering Offences

The Proceeds of Crime Act 2002 (POCA) and the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 broadened the definition of money laundering.

1. Primary Money Laundering Offences:

There are a number of different offences that may be committed under the applicable legislation:

- Concealing, disguising, converting, transferring or removing criminal property from the UK (Section 327 POCA);
- Entering into or becoming concerned in an arrangement which a person knows or suspects facilitates the acquisition, retention, use or control of criminal property (Section 328 POCA);
- Acquiring criminal property, using criminal property; or possession of criminal property (Section 329 POCA).
- Doing something that might prejudice an investigation into money laundering (for example, falsifying a document) (Section 342 POCA).

The above are the primary Money Laundering offences, and are prohibited under the legislation. A person does not commit an offence under Sections 327 – 329 of POCA if they made an authorised disclosure before they did the act and had consent, or if they intended to make disclosure but have a reasonable excuse for not doing so. This provision emphasises the importance of reporting possible money laundering instances to the National Crime Agency.

2. Secondary Money Laundering Offences:

There are also two secondary offences, which only apply to public authorities like Cambridgeshire County Council if they are undertaking activities which fall into the 'regulated sector' under POCA. This includes a range of business activities, generally where persons are handling money on behalf of others, such as certain accountancy or legal services.

The secondary offences are:

- Failure to disclose/report any of the three primary offences (Sections 330 and 331 of POCA) - when a person knows or suspects that money laundering activity is taking

place (or has taken place), or becomes concerned that their involvement in a matter may amount to a prohibited act under the legislation, they must report this as soon as practicable to the Money Laundering Responsible Officer (MLRO) or risk prosecution.

- Tipping off (Section 333A) – this is where someone informs a person, or people, who are suspected of being involved in Money Laundering, in such a way as to reduce the likelihood of their being investigated, or prejudicing an investigation.

3. Terrorism Act Offences:

The Terrorism Act (TACT) made it a money laundering offence to enter into or become concerned in an arrangement relating to the retention or control of property likely to be used for the purposes of terrorism, or resulting from acts of terrorism. All individuals and businesses in the UK have an obligation to report knowledge, reasonable grounds for belief or suspicion about the proceeds from, or finance likely to be used for, terrorism, where it relates to information that comes to them in the course of their business or employment.