



# Anti-Money Laundering Policy

Document Owner	Version
<b>Vicky Chuter, Financial Reporting Manager, Corporate Finance</b> Tel: 03302 223414 Vicky.chuter@westsussex.gov.uk	Version 2

## Document Review History

Version	Reviewed	Reviewer	Approver	Date approved
Original			RAAC	14 November 2005
1			RAAC	28 November 2016
2	May 2023	Vicky Chuter	RAAC	
Next Review Date	June 2026			

## **Anti-Money Laundering Policy**

West Sussex County Council will do all it can to prevent the Council and its staff being exposed to money laundering, to identify the potential areas where it may occur, and to comply with all legal and regulatory requirements, especially for the reporting of actual or suspected cases.

### **Key Points**

- The Council is committed to the prevention, detection and reporting of money laundering
- All Members and staff must be vigilant for the signs of money laundering
- Any employee who suspects money laundering activity must report this promptly to the Money Laundering Reporting Officer
- No payment to the Council will be accepted in cash if it exceeds £5,000
- Cumulative cash payments reaching £5,000 or more from a single source will be examined to assess the risk of money laundering.
- Where the Council is carrying out relevant business the Client Identification Procedure must be followed (see Appendix A, Section 2).

### **1. Introduction**

- 1.1. West Sussex County Council (WSCC) 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) 2002, the Terrorism Act 2000 and the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 place obligations on WSCC and its employees to ensure that procedures are in place to prevent the Council's services, contracts or financial transactions being used for money laundering.
- 1.3. The requirements of WSCC of the legislation are:
  - To appoint a money laundering reporting officer (Nominated Officer)
  - Implement a procedure to receive and manage the concerns of staff about money laundering and their suspicion of it, and to submit reports where necessary, to the National Crime Agency (NCA)
  - To make those staff most likely to be exposed to money laundering situations aware of the requirements and obligations placed on the organisation, and on them as individuals
  - To give targeted training to those considered to be the most likely to encounter money laundering.
- 1.4. This Policy sets out the process to fulfil the requirements of the legislation and minimise the risk, as well as provide guidance on the Council's money laundering procedures which are set out in Appendix A. Adhering to this Policy and guidance will protect employees from the risk of prosecution if they become aware of money laundering activity while employed by the Council.

- 1.5. 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. The Council's Policy is to do all it can to prevent, wherever possible, the Council and its staff being exposed to money laundering, to identify the potential areas where it may occur, and to comply with all legal and regulatory requirements, especially with regard to the reporting of actual or suspected cases. All staff have a responsibility to be vigilant.

## **3. Scope of the Policy**

- 3.1. This Policy applies to Members and all employees of the Council. It aims to maintain the high standards of conduct which currently exist within the Council by preventing criminal activity through money laundering. The Policy sets out the procedures, in Appendix A, which must be followed to enable the Council to comply with its legal obligations.
- 3.2. This Policy sits alongside the Council's Anti-Fraud and Corruption Strategy.
- 3.3. Failure by a member of staff to comply with the procedures set out in this Policy may lead to disciplinary action being taken against them. Any disciplinary action will be dealt with in accordance with the Council's Disciplinary Policy.

## **4. What is money laundering?**

- 4.1. Money laundering is the term used for a number of offences involving the proceeds of crime or terrorism funds. The following acts constitute money laundering:
  - concealing, disguising, converting, transferring criminal property and cash, or removing it from the UK (section 327 of the Proceeds of Crime Act 2002);
  - 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);
  - acquiring, using or possessing criminal property (section 329);
  - becoming concerned in an arrangement facilitating concealment, removal from the jurisdiction, transfer to nominees or any other retention or control of terrorist property (section 18 of the Terrorism Act 2000), that will benefit a terrorist organisation.
- 4.2. These are the primary money laundering offences and are thus prohibited by law. There is also a secondary offence: failure to disclose any of the four primary offences.

- 4.3. Any Member or member of staff could potentially be caught by these money laundering provisions, if they suspect money laundering and either become involved with it in some way and/or do nothing about it. This Policy sets out how any concerns should be raised.
- 4.4. While the risk to the Council of contravening the legislation is low, it is important that all employees are familiar with their responsibilities as 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.

## **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 Appendix A for a list of areas that may be affected. Although you do not need to have 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 or suspicious, 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,
  - Overpaying invoices and then asking for cash refunds, or
  - Unusual property transactions or unusual transfer of assets or funds.
- 5.3. Any transaction or series of transactions 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 Money Laundering Reporting Officer (MLRO)**

- 6.1. The officer nominated to receive disclosures about money laundering activity within the Council is the Financial Reporting Manager.

Contact details are as follows:

Vicky Chuter  
Financial Reporting Manager  
West Sussex County Council  
County Hall  
Chichester  
West Sussex  
PO19 1RQ  
Telephone: 03302 2223414

E-mail: [vicky.chuter@westsussex.gov.uk](mailto:vicky.chuter@westsussex.gov.uk)

## **7. Further Information**

7.1. Further information can be obtained from the following sources:

- National Crime Agency (NCA) - [Money laundering and illicit finance - National Crime Agency](#)
- Combating Financial Crime: Practical Advice for the Public Sector (2020 Edition)
- "Proceeds of Crime (Anti-Money Laundering) – Practical Guidance for Public Service Organisations" – CIPFA
- Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017
- "Anti-Money Laundering (Proceeds of Crime and Terrorism) – Second Interim Guidance for Accountants" – CCAB ([www.ccab.org.uk](http://www.ccab.org.uk))
- Money Laundering Guidance at [www.lawsociety.org.uk](http://www.lawsociety.org.uk)
- HMRC - <https://www.gov.uk/report-tax-fraud>

## **8. Conclusion & Risk Assessment**

8.1. The risk of WSCC being exposed to money laundering is currently considered to be low. This assessment is based on the low amount of cash the Council receives from income sources, low volumes and low amounts of refunds being made and the controls that we have in place relating to asset transfers, contracts and property transactions. However, failure to comply with legislation and the relevant guidance by individuals could lead to prosecution, so continual vigilance and compliance is essential.

## Anti-Money Laundering Procedures

### 1. Reporting Concerns

- 1.1. Any employee who suspects money laundering activity must report their suspicion promptly to the Money Laundering Reporting Officer (MLRO), or to the MLRO's deputy if appropriate, using the attached form (Appendix B). If you would prefer, you can discuss your suspicions with the MLRO or their deputy first.
- 1.2. The employee must follow any subsequent directions of the MLRO or deputy and must not themselves make any further enquiries into the matter. They must not take any further steps in any related transaction without authorisation from the MLRO.
- 1.3. The employee must not disclose or otherwise indicate their suspicions to the person suspected of the money laundering. They must not discuss the matter with others or note on the file that a report has been made to the MLRO in case this results in the suspect becoming aware of the situation.
- 1.4. The MLRO or deputy must promptly evaluate any report of potential money laundering, to determine whether it should be reported to the National Crime Agency (NCA)<sup>1</sup>.
- 1.5. The MLRO or deputy must, if they so determine, promptly report the matter to NCA. The NCA website is at [Suspicious Activity Reports - National Crime Agency](#)
- 1.6. The MLRO or deputy will commit a criminal offence if they know or suspect, or have reasonable grounds to do so, through a disclosure being made to them, that another person is engaged in money laundering and they do not disclose this as soon as practicable to the NCA.

### 2. Responsibility of employees

- 2.1 All employees have a responsibility to be vigilant for potential money laundering activities when transacting with third parties. Alongside the internal controls in place to minimise the potential for money laundering, staff should continue to be aware of this risk. Where the Council is carrying out 'relevant business'<sup>2</sup> and, as part of this:
  - forms an on-going business relationship with a person or organisation; or
  - undertakes a one-off transaction involving cash payments by or to the other(s) of £5,000 or more; or
  - undertakes a series of linked one-off transactions involving total payment by or to the other(s) of £5,000 more; or

---

<sup>1</sup> formerly the Serious Organised Crime Agency (SOCA).

<sup>2</sup> The Act defines Relevant business as the provision 'by way of business' of: advice about tax affairs; accounting services; audit services; legal services involving financial or real property transactions; 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 Sterling equivalent) or more.

- it is known or suspected that a one-off transaction (or a series of them) involves money laundering;

then the procedure (as set out below) must be followed before any business is undertaken for that client.

2.2 Where the 'relevant business' is being provided to another public sector body you must ensure that you have signed, written instructions on the body's headed paper before any business is undertaken.

2.3 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 or operating from a country or foreign jurisdiction considered to be unusual or unfamiliar, or where the transaction is complex or unusually large.

### 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 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	<ul style="list-style-type: none"> <li>• Selling property to individuals or businesses</li> <li>• Renting out property to individuals or businesses</li> <li>• Entering into other lease agreements</li> <li>• Undertaking services for other organisations</li> </ul>
Secretive clients	<ul style="list-style-type: none"> <li>• People buying or renting property from the Council who may not want to say what it is for</li> <li>• People receiving grant funding who refuse to demonstrate what funding was used for</li> </ul>
Customers who we think are acting dishonestly or illegally	<ul style="list-style-type: none"> <li>• People paying for Council services who do not provide details about themselves</li> <li>• People making odd or unusual requests for payment arrangements</li> </ul>

<b>Activity</b>	<b>The types of activity that may be affected</b>
Illogical transactions	<ul style="list-style-type: none"> <li>• People paying in cash then requesting refunds</li> <li>• Requests for the Council to pay seemingly unconnected third parties in respect of goods / services provided to the Council</li> <li>• Requests for the Council to pay in foreign currencies for no apparent reasons</li> </ul>
Payments of substantial sums by cash	<ul style="list-style-type: none"> <li>• Large debt arrears paid in cash</li> <li>• Refunding overpayments</li> <li>• Deposits / payments for property</li> </ul>
Movement of funds overseas	<ul style="list-style-type: none"> <li>• Requests to pay monies overseas, potentially for "tax purposes"</li> </ul>
Cancellation of earlier transactions	<ul style="list-style-type: none"> <li>• Refunds for services no longer needed / used. Extra vigilance is required if payment request is not to the original payee.</li> <li>• No payment demanded even though good / service has been provided. Possible unwillingness to share bank details.</li> <li>• Sudden and unexpected termination of lease agreements. These can be suspicious, as formal leases can legitimise company addresses and cash flows.</li> </ul>
Requests for client account details outside normal course of business	<ul style="list-style-type: none"> <li>• Queries from other companies regarding legitimacy of customers</li> <li>• Council receiving correspondence / information on behalf of other companies</li> </ul>

#### **4. Record Keeping**

3.2 Where 'relevant business' is carried out the client identification evidence and details of the relevant transaction(s) for that client must be retained for at least five years.

#### **4 Monitoring Arrangements**

4.1 An annual review of key service areas will be undertaken in order to gain assurance that adequate monitoring arrangements are in place and that any potential money laundering activity has been identified and appropriate action taken.

#### **5. Guidance and Training**

5.1 In support of the policy and procedure, the Council will:

- make all staff aware of the requirements and obligations placed on the Council and on themselves as individuals by the anti-money laundering legislation; and
- targeted training for those most likely to encounter money laundering.



## Disclosure Report to Money Laundering Reporting Officer

### 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:	
Reason for Association:	
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:	
Account number	
Sort Code	
Current Balance	
Balance Date	

Account Holder's Name:	
Account number	
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:	
Continued:	
Continued	
Type: (Home, Work, etc)	

**Reason for Suspicion:**

Please enter details of your suspicions. Please provide as much information as possible, overleaf.

