

**The Moray Council**  
**Corporate Governance**  
**Anti Money Laundering Policy**

Owner of Policy	Chief Financial Officer
Author	Lorraine Paisey
Date of Review	August 2023
Date of previous version	
Policy Approved	
Next Review Date	December 2026

# Anti Money Laundering Policy

## 1. Introduction

This policy explains money laundering and the legal and regulatory framework in place to govern its disclosure. It also specifies the processes that need to be adopted to ensure as far as practicable that the Council and its employees are not exposed to money laundering. The policy complements the *Policy to Combat Fraud, Theft, Bribery and Corruption and Treasury Management Practice Note 9* which considers money laundering in the context of treasury management.

The Council has limited its direct exposure to laundering of cash by arranging for collection of significant income streams either electronically or at external collection points. Separately, procurement procedures ensure that appropriate steps are taken to establish the identity and standing of Council suppliers and contractors. The risk of the Council contravening the legislation is therefore considered to be relatively low.

The Chartered Institute of Public Finance and Accountancy (CIPFA) has published guidance to advise public service organisations what they should do to combat financial crime of this type.

## 2. Money Laundering Regulations

Money laundering is the process by which the proceeds of crime or terrorism funds are changed so that they appear to come from a legitimate source. The legal and regulatory provisions that cover money laundering are as follows:

- The Proceeds of Crime Act 2002 (POCA)
- The Terrorism Act 2000 (TA)
- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017
- Money Laundering and Terrorist Financing (Amendment) Regulations 2019

The POCA defines the primary money laundering offences, and thus prohibited acts, as

1. Concealing, disguising, converting, transferring or removing criminal property from the UK (section 327)
2. Being concerned in an arrangement which a person knows or suspects facilitates the acquisition, retention, use or control of criminal property (section 328)
3. Acquiring, using or possessing criminal property (section 329)
4. Doing something that might prejudice an investigation – for example falsifying a document (section 342)

The TA places an obligation on all individuals and businesses in the UK to report knowledge, reasonable grounds for belief or suspicion about the proceeds from, or finance likely to be used for, terrorism or its laundering,

where it relates to information that comes to them in the course of their business or employment.

The CIPFA guidance on the application of legal and regulatory provisions to public authorities notes that the Council and its employees are subject to the full provisions of the TA and to the four POCA offences outlined above.

There are two further POCA offences relating to failure to disclose (under section 330 and 331) and to 'tipping off' (informing a suspect) (under new section 333a) but so long as the Council does not undertake activities which might be interpreted under POCA as falling within the regulated sector, the offences of failure to disclose and tipping off do not apply. The regulated sector refers to activities that are regulated under the Financial Services and Markets Act 2000.

The 2017 Regulations refer to 'relevant businesses' and 'relevant persons'. Local authorities are not listed and therefore are not subject to the requirements of the 2017 regulations

### **3. Council responsibilities**

CIPFA's view is that it is prudent and responsible practice for all public sector organisations, including those outwith the scope of the Regulations, to put in place appropriate and proportionate money laundering arrangements designed to enable them to detect and avoid involvement in the crimes described in the legislation and regulations.

The arrangements for this Council cover

- Specifying the scope and coverage of the policy
- Nomination of a Money Laundering Reporting Officer
- Development of relevant procedures

### **4. Scope and Coverage of the Policy**

The principal concern for the Council with regard to money laundering apart from an employee being involved in a criminal act is the risk of suspicious activity not being reported to the Serious and Organised Crime Agency (SOCA).

The Council therefore will do all it can to prevent the organisation and its staff being exposed to money laundering and to comply with all legal and regulatory requirements, especially with regard to the reporting of actual or suspected cases. It should be recognised that serious criminal sanctions may be imposed for breaches of the legislation therefore it is important that all employees and elected members are familiar with this policy and report any suspected money laundering activity promptly.

## **5. Nomination of a Money Laundering Reporting Officer (MLRO)**

To secure effective central reporting and recording of disclosures in relation to suspected money laundering the Council has nominated the Chief Financial Officer as its MLRO. The Chief Financial Officer will be responsible for the development and maintenance of relevant procedures.

## **6 Relevant Procedures**

A reporting framework to log any potential money laundering incidents has been established. This ensures there is a channel for suspicions to be raised and for these to be dealt with in a consistent manner. Reporting proformas are available from Financial Services.

Where money laundering activity is suspected by any elected member or employee, details should be reported to the MLRO using the prescribed form. If preferred, suspicions can be discussed with the MLRO in the first instance.

The person reporting the concern must follow any directions of the MLRO 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.

The MLRO must promptly evaluate any reports received to determine if a report to SOCA is necessary. The MLRO must, if they so determine, promptly report the matter to SOCA on their standard report form and in the prescribed manner. Up to date forms can be downloaded from the SOCA website.

All persons making reports are required to co-operate with the MLRO or an officer nominated by the MLRO during any subsequent investigation, and at no time and under no circumstances should any suspicions be voiced to the person or persons suspected of the money laundering, even where SOCA has given consent to a particular transaction proceeding.

Examples of how money laundering may occur and details of how suspicions should be recorded and reported are provided in a guidance note for employees. There is no single flag which would identify money laundering, however, the following may, in some cases, be an indication of money laundering activity:

- Use of cash where other means of payment are normal
- Overpayments by a customer
- Unusual request for cancellation or reversal of an earlier transaction
- Customer requesting refunds to be transferred overseas, particularly to a high risk country or tax haven
- Payments of lower amounts where cash is not the usual means of payment
- Use of new/shell companies
- A secretive customer, for example, one who refuses to provide the requested information without a reasonable explanation
- Illogical customer transaction such as 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

- Absence of an obvious legitimate source of funds
- Concern about the honesty and integrity of the customer
- Unusual transaction or way of conducting business without reasonable explanation
- Unusual transactions or ways of conducting business
- Individuals and companies which are insolvent yet have funds
- Transaction at substantially above fair market value
- Funds received for deposits or before completion from unexpected sources

There is also a need to consider 'customer due diligence', which essentially requires that proportionate steps are taken to establish the identity of any individual or organisation that wishes to do business with the council.

In any set of circumstances employees are asked to consider

Who they are dealing with –someone they know or a stranger

How freely requests for information is given

Prior knowledge of the person's dealings with the Council

How usual the transaction is in terms of size, nature and frequency

Any unusual or illogical involvement of third parties/ third party funds

The absence of an obvious legitimate source of funds

Involvement of agents e.g. solicitors who are geographically remote

To mitigate the risk of money laundering through the council, cash payments (notes or coins) exceeding £300 shall not be accepted. This figure has been set at a level reflecting the current situation where the council no longer operates its own cash collection offices and thus has limited responsibilities for physically handling cash.

(1062742)