



Doncaster  
Council

# **Doncaster Council**

## **Anti-Money Laundering Policy**

## Contents

1. Introduction .....	3
2. Scope of the policy .....	3
3. Relevant legislation applicable to this policy.....	3
4. What is “money laundering”? .....	4
5. What are the Council’s obligations? .....	5
6. Money laundering – higher risk activities .....	5
7. Warning signs of potential money laundering .....	7
8. What do I need to do to comply? .....	7
9. Due diligence checks .....	8
10. Reporting suspicions to the Money Laundering Reporting Officer .....	11
11. Consideration of the report by the Money Laundering Reporting Officer .....	12
12. Record keeping and record retention .....	13
13. Data protection considerations .....	15
14. Freedom of information considerations .....	15
15. Review of this policy .....	16

## **1. Introduction**

- 1.1. The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (known throughout this policy as MLR 2017) came into force on 26 June 2017. They implement the EU's 4th Directive on Money Laundering. In doing so, they replace the Money Laundering Regulations 2007 and the Transfer of Funds (Information on the Payer) Regulations 2007 which were previously in force.
- 1.2. This policy is designed to set out the Council's approach to money laundering prevention and associated reporting. This document should be read in conjunction with the Whistleblowing Policy and the Anti-Fraud, Bribery and Corruption Frameworks.

## **2. Scope of the policy**

- 2.1. This policy applies to all employees of the Council, whether temporary or permanent, and any agents acting on behalf of the Council. This policy is also applicable to elected members where any suspicions of money laundering activity are noted or come to light.
- 2.2. This Policy 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, which must be followed to enable the Council to comply with its legal obligations.

## **3. Relevant legislation applicable to this policy**

- 3.1. The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (*MLR 2017*).
- 3.2. The Proceeds of Crime Act (*POCA*) 2002.
- 3.3. A "*Money Laundering Reporting Form*" accompanies this document.

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

- 4.1. Money laundering is the method by which cash or funds obtained illegally are passed or “laundered” through financial systems to disguise their criminal origin. The “laundered” funds can then be used for legitimate transactions that do not arouse suspicion. It is a favoured method of organised criminals and terrorists.
- 4.2. The term “Money Laundering” describes offences involving the integration of the proceeds of crime, or terrorist funds, into the mainstream economy. Such offences are defined under The Proceeds of Crime Act 2002 as the following prohibited acts;
- Concealing, disguising, converting, transferring or removing criminal property from the UK.
  - Becoming involved in an arrangement which an individual knows or suspects facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person.
  - Acquiring using or possessing criminal property.
  - Doing something that might prejudice an investigation e.g. falsifying a document.
  - Failure to disclose one of the offences listed above where there are reasonable grounds for knowledge or suspicion.
  - Tipping off a person(s) who is suspected of being involved in money laundering in such a way as to reduce the likelihood of or prejudice an investigation.
- 4.3. Money laundering activity may range from a single act such as the use of criminal funds to pay an invoice to multiple payments to an account to “launder” money in smaller chunks to avoid checks and suspicions. They can even involve sophisticated schemes involving multiple parties and multiple methods of handling and transferring criminal property, as well as concealing it, and entering into arrangements to assist others to do so. Council employees need to be alert to the risks of money laundering in any of its many forms.



## **5. What are the Council's obligations?**

- 5.1. Whilst Local Authorities are not directly covered by the requirements of the Money Laundering Regulations 2017, guidance from finance and legal professions, including the Chartered Institute of Public Finance and Accounting (CIPFA), indicates that public service organisations should comply with the underlying spirit of the legislation and regulations and put in place appropriate and proportionate anti-money laundering safeguards and reporting arrangements.
- 5.2. The obligations on the Council are to establish and maintain appropriate and risk-sensitive policies (after a documented risk assessment) and procedures relating to the following;
- Customer due diligence measures (checks) and ongoing monitoring of financial transactions;
  - Reporting of suspected money laundering activities;
  - Appropriate record keeping; and
  - The appointment of a named Money Laundering Reporting Officer.

## **6. Money laundering – higher risk activities**

- 6.1. The Council does not normally in the course of most of its duties undertake “regulated activities” for which additional checks and measures are necessary (these additional measures are known as “*due diligence*” checks). However, some Council activities are considered to be higher risk. On such transactions we must ensure that we comply with the spirit of the money laundering regulations. These activities include (but are not limited to):
- Any advice given on tax affairs or accounting / auditing services done for other parties;
  - Legal services;

- Property sales (commercial and those of housing stocks)
- The handling of any transaction involving a cash payment of €15,000 or more. (Cash is defined as “notes, coins or travellers’ cheques in any currency”). It is the Council’s policy not to accept more than £11,000 in cash in any single transaction. However, cumulatively, cash transactions may exceed this level if not properly monitored (it should be noted however, that this is extremely unlikely). For this reason, the Council has adopted a risk based approach and will undertake appropriate checks on any cash transactions (single or cumulative) of £10,000 or more.

6.2. All employees need to be aware of the possibility of money laundering in their day to day activities. The following scenarios illustrate how money laundering risks are part of our everyday activities:

6.2.1. A social worker is assessing a service user's finances to calculate how much they should pay towards the cost of their care, and then goes on to arrange for services to be provided and charged for. If the service user's finances are the result of criminal activities, the social worker could be committing a prosecutable offence if they know or suspect that the monies are not legitimate income and does not report their concerns.

6.2.2. The Council (via the Director of Adult Services) are court appointed deputies for a service users financial and property affairs. If the member of staff in the Safeguarding Adults Personal Assets Team dealing with the discharge of those responsibilities, notices unusual income being received by the individual either in the past or on an ongoing basis and does not report those concerns for investigation; they may be committing an offence.

6.2.3. In the course of the sale of a Council property (commercial or a council house), the Right to Buy and / or Legal Services team become aware that the buyer wishes to pay a substantial amount in cash (either to fund the property or the deposit), then those dealing with the sale may be

committing an offence if sufficient checks are not undertaken and the property purchase ends up funded from the proceeds of criminal activity.

6.2.4. An employee notices unusual transactions made on the account of the debtor (for example a Business Rates debtor) in that relatively large amounts of cash are being paid to an account or the account being overpaid and a refund requested. These accounts may be under the €15,000 limit, however, if the pattern of payments suggests money laundering (or the monies are coming from different and unusual sources), the employee may be committing an offence if they do not report the suspicious transactions for further investigation.

## **7. Warning signs of potential money laundering**

7.1. Criminals have various ways of concealing, moving and legitimising the proceeds of their crimes. This policy cannot list every potential scenario that could indicate money laundering however, some potential warning signs include:

- the use of cash where other means of payment are more normal (unusual transactions);
- an unwillingness on behalf of the customer to answer questions / secretiveness;
- the use of shell or intermediary companies or persons to pass the monies on to us (such as money through different customers in different names);
- the payment of monies that are then requested back;
- overpayments received that are subsequently requested for a refund;
- individuals or companies that appear insolvent (appear not to have funds) that are making transactions or are making transactions that appear beyond their means;
- the involvement of a third party in a transaction without obvious cause or need; or

- the movement or coming of funds from a different country;

## **8. What do I need to do to comply?**

- 8.1. It is the responsibility of services managers to ensure that their systems of internal control are robust and that their staff are appropriately trained in respect of money laundering. It is also the responsibility of service managers to ensure that appropriate due diligence checks are undertaken on any relevant transactions (see section 8 for further explanations).
- 8.2. Where you are involved in a higher risk transaction or become aware of the transfer of significant amounts (£10,000+) cash (either as a single or multiple transactions), you must undertake due diligence checks to ensure that you know who your customer is and that the monies are legitimate. (See section 9 below). It is the policy of the Council not to accept single cash payments over €15,000 or the UK monetary equivalent (approximately £11,000). However, some sales such as Right to Buy sales will be purchased by electronic bank transfer. Despite these not being a true “cash” payment, it is still important to undertake the proper due diligence checks on the source of any funds being used to make the purchase despite the electronic method of transfer.
- 8.3. Where you, as either an individual or a team, suspect (or know) that money laundering activity is taking place then you must report it to the Money Laundering Reporting Officer and obtain advice and permission to continue the transaction.
- 8.4. IF YOU FAIL TO REPORT ANY SUSPICIONS YOU MAY BE LIABLE TO PROSECUTION.**
- 8.5. You must follow any advice or instructions given by the Money Laundering Reporting Officer. For Doncaster Council, this is the Chief Financial Officer and Assistant Director of Finance. (Further details on how to do this can be found in section 9).

## **9. Due diligence checks**

9.1. Due diligence is the name given to the additional checks undertaken in higher risk transactions (as outlined earlier). These checks ensure that the Council understands its customer and its business so that the Council is in a position to know if any suspicious activity needs to be reported.

9.2. MLR 2017 requires that;

- the Council identifies its customer and verifies that identity based on documentation and data obtained from a reliable source.
- the Council identifies, where there is a beneficial owner who is not the customer and taking adequate measures, on a risk-basis, to verify their identity so that we know who we are ultimately dealing with. This may be because someone else is acting on behalf of another person in a particular transaction, or it may be that we need to establish the ownership structure of a company, partnership or trust. As a general rule, the beneficial owner is the person who's behind the customer and who owns or controls the customer; Or it's the person on whose behalf a transaction or activity is carried out.
- the Council obtains information on the purpose and intended nature of the business relationship. This means understanding where the funds are coming from and the real purpose of the transactions.
- In addition to the above, if the transaction involves dealing with a person from a high risk 3rd country (as defined by the European Union), enhanced due diligence and additional risk assessment is necessary. A full list of high risk jurisdictions is available on [www.gov.uk](http://www.gov.uk), however, at the time of review this includes: Afghanistan, Bosnia and Herzegovina, Guyana, Iraq, Lao Peoples Democratic Republic, Syria, Uganda, Vanuatu, Yemen, Iran and the Democratic People's Republic of Korea.

9.3. To undertake these checks you should:

- 9.3.1. Check your customer's identity, specifically their name, address, date of birth, using official photographic documentation. The best way to do this is to ask for a government issued document like a passport, along with utility bills, bank statements and other official documents. Other sources of customer information include information held by credit reference agencies such as Experian and Equifax (although this information must be checked with their consent). If you have doubts about a customer's identity, you must not continue to deal with them until you are sure.
- 9.3.2. If you are dealing with a company or trust and not an individual, you will need to determine who owns the trust / company to determine who your customer really is. Please seek additional advice from Internal Audit Services if you are unsure of how to do this.
- 9.3.3. You will need to determine the source and origin of funds that your customer will be using in the relationship / transaction, especially where this is a cash transaction. This will involve requesting and reviewing copies of recent and current financial statements and reviewing the source of the cash being used. In the event of a property sale or right to buy application the source of the funds will still need to be investigated. Where a mortgage is being put in place, you will need to review the "mortgage offer in principle" to confirm the source of the funds. Where the investment is coming from a business, you will need to understand the ownership of that business and any related parties to it.
- 9.3.4. You will also need to understand the relationships between any joint parties, for example where 2 people are purchasing a property or council house, you will need to understand the relationship between the parties to ensure that money laundering (or fraud) is not taking place.
- 9.4. The checks described above must generally be undertaken by the Council before it establishes a business relationship or carries out an occasional transaction, or if it suspects money laundering or terrorist funding or doubts the veracity of any information obtained for the purposes of identification or verification. However, the Council is not required to undertake these checks if its

customer is another public authority, unless it suspects money laundering or terrorist funding.

9.5. Enhanced checks (over and above those described above) are necessary where:

- the customer is not physically present when you carry out identity checks;
- when you enter into a relationship or transaction with 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);
- where you enter into a transaction with someone from a 3<sup>rd</sup> risk country (as outlined in paragraph 8.2, point 3); or
- you feel that there is a high risk for money laundering.

9.6. In all of these cases additional checks are necessary and you should contact the Money Laundering Reporting Officer or their representative for additional guidance before undertaking additional checks.

9.7. Should any of your checks arouse suspicions, you must stop the transaction / dealing with the customer and report the activity immediately using the details in the next section. **Should you fail to do so, you may be liable to prosecution and disciplinary action.**

## **10. Reporting suspicions to the Money Laundering Reporting Officer**

10.1. The officer nominated to receive disclosures about money laundering activity within the Council is the Chief Financial Officer and Assistant Director of Finance.

10.2. Where you know or suspect that money laundering activity is taking/has taken place, you must disclose this as soon as practicable to the Money Laundering Reporting Officer. The disclosure should be within hours of the information coming to your attention, not weeks or months later. **DO NOT** attempt to make further investigations into the matter yourself.

- 10.3. Your disclosure should be made to the Money Laundering Reporting Officer using the Money Laundering Suspensions Reporting Form giving as much detail as is possible. If you prefer, you can discuss the matter with the Money Laundering Reporting Officer first. You must follow any advice or instructions issued by the Money Laundering Reporting Officer.
- 10.4. Once you have reported the matter to the Money Laundering Reporting Officer you must follow any directions he may give you. You **MUST NOT** make any further enquiries into the matter yourself; simply report your suspicions to the Money Laundering Reporting Officer who will refer the matter on to the National Crime Agency (NCA) if appropriate. All members of staff will be required to co-operate with the Money Laundering Reporting Officer and the authorities during any subsequent money laundering investigation.
- 10.5. Similarly, at no time and under no circumstances should you voice any suspicions to the person(s) whom you suspect of money laundering, otherwise you may commit a criminal offence yourself in “tipping off” the reported person.
- 10.6. **DO NOT**, therefore, make any reference on a client file to a report having been made to the Money Laundering Reporting Officer. Under data protection legislation the customer can exercise their right to see their file (a Data Subject Access Request) at any point in time. Such a note will obviously tip them off to the report having been made. The Money Laundering Reporting Officer will keep the appropriate records in a confidential manner.
- 10.7. Should any investigation be necessary (in conjunction with the National Crime Agency), you will be required to participate and supply information as appropriate under the direction of the Money Laundering Reporting Officer.

## **11. Consideration of the report by the Money Laundering Reporting Officer**

11.1. The Money Laundering Reporting Officer will consider the report and any other available internal information they think is relevant e.g.:

- reviewing other transaction patterns and volumes;
- the length of any business relationship involved;

- the number of any one-off transactions and linked one-off transactions; and
- any identification evidence held.

11.2. The Money Laundering Reporting Officer will undertake such other reasonable inquiries he thinks appropriate in order to ensure that all available information is taken into account in deciding whether a report to the National Crime Agency is required (such enquiries being made in such a way as to avoid any appearance of tipping off those involved). The Money Laundering Reporting Officer may also need to discuss the report with you.

11.3. Once the Money Laundering Reporting Officer 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; or
- there are reasonable grounds to know or suspect that is the case; and
- whether they need to seek consent from the National Crime Agency for a particular transaction to proceed.

11.4. Where the Money Laundering Reporting Officer does conclude that there are reasonable grounds to suspect money laundering, then they must disclose the matter as soon as practicable to the National Crime Agency on their standard report form and in the prescribed manner, and await their instructions.

11.5. Where the Money Laundering Reporting Officer concludes that there are no reasonable grounds to suspect money laundering then they will mark the report accordingly and give consent for any on-going or imminent transaction(s) to proceed.

## **12. Record keeping and record retention**

12.1. Each department undertaking due diligence checks **MUST** maintain records of the checks carried out including copies of any evidence obtained to support the transactions / due diligence assessment.

- 12.2. The precise nature of the records is not prescribed by law; however, they must be capable of providing an audit trail during any subsequent investigation.
- 12.3. On **NO ACCOUNT** should a record of or any mention of, any referrals to the Money Laundering Reporting Officer be kept / mentioned on a customer's file. The file must not contain details of any such suspicions as the file can be reviewed by the customer at any time and it is important that the customer is not "tipped off" about any allegations accidentally.
- 12.4. Records must be kept for a minimum of 5 years to allow for any investigation to take place.
- 12.5. A record of the destruction of such information (including the money laundering reporting form) must also be kept in line with normal Council procedures.
- 12.6. An electronic copy of every customer due diligence record must be sent to the Money Laundering Reporting Officer to meet the requirements of the Regulations and in case of inspection by the relevant supervising body.

### **13. Data protection considerations**

- 13.1. Under data protection regulations any customer may ask to see the information that we hold about them. This is called a Data Subject Access Request. Under the law, we must provide this information. However, the regulations (both the General Data Protection Regulation and its predecessor) contain exemptions.
- 13.2. Exceptions apply in this case, where the release of the data would likely prejudice the prevention and detection of a crime or would cause the body releasing the information to actually commit a crime in doing so. As a result, money laundering referrals are usually exempt from any such subject access request, which is why the referral should not be documented on the customer's file. However, this does not prevent the release of all of the customer's information. Advice on the application of exemptions in this respect should be taken before any release of the information takes place.

### **14. Freedom of information considerations**

- 14.1. The Freedom of Information Act 2000 gives members of the public a general right of access to all types of recorded information held by public authorities, which includes the Council. The general right of access is, however, subject to exemptions.
- 14.2. The relevant exemptions are contained in section 23 (information supplied by, or relating to, bodies dealing with security matters) and section 31 (law enforcement). Information is exempt from disclosure if it would likely prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.
- 14.3. Summary information, i.e. the number of reported suspicions, may be releasable providing that individual customers / referrals cannot be identified. In all cases, advice should be sought before dealing with any Freedom of Information request relating to money laundering activities.

**15. Review of this policy**

15.1. This policy will be reviewed annually and is next due for review in March 2019.

15.2. All significant amendments will be subject to approval by the Audit Committee.

<b>Version</b>	<b>Date of Amendment / Review</b>	<b>Details of Amendments</b>
1.0	November, 2013	Initial publication
2.0	July, 2018	Amendment to incorporate The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017  Introduction of the Money Laundering Fact Sheet