W

Wirral Council

Anti-Money Laundering Policy

Wirral Internal Audit Service
July 2018

1 Introduction

1.1 The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017) came into force on 26 June 2017. They implement the EU's 4th Directive on Money Laundering and in doing so they replace the Money Laundering Regulations 2007 (MLR 2007) and the Transfer of Funds (Information on the Payer) Regulations 2007, which were previously in force.

1.2 A key difference in the Regulations is to require "relevant persons" to adopt a more risk-based approach towards anti-money laundering, in particular in how they conduct due diligence. Determining the appropriate level of due diligence requires analysis of risk factors based on the EU Directive and which are set out in MLR 2017, as detailed in section 8 of this Policy .

2 Scope of the Policy

2.1 This Policy applies to all Members, employees, partners and external bodies working on behalf of the Council and aims to maintain the high standards of conduct which currently exist within the Council by reducing the risk of criminal activity through money laundering. The Policy sets out the procedures which must be followed (for example the reporting of suspicions of money laundering activity) to enable the Council to comply with its legal obligations.

2.2 The Policy sits alongside the Council's Anti-Fraud and Corruption Policy, Anti-Bribery Policy, and Whistle-blowing Policy.

2.3 There is an accompanying briefing note to this policy which will act as a quick reference guide to inform front line employees of the fundamental areas of the policy that apply to them (See Appendix 1).

2.4 Failure by an employee, Member partner or an external body working on behalf of the Council to comply with the procedures set out in this Policy could result in them committing a criminal offence. Therefore, it is extremely important that all individuals working on behalf the council are familiar with their legal responsibilities.

3 What is Money Laundering ?

3.1 Money Laundering is the term used for a number of offences involving the integrating of "dirty money'' (i.e. the proceeds of crime) into the mainstream economy. The objective of which is to legitimise the possession of such monies through circulation and this effectively leads to "clean'' funds being received in exchange.

3.2 Such offences are defined under The Proceeds of Crime Act 2002 (POCA) as the following prohibited acts:

- Concealing, disguising, converting, transferring or removing criminal property from the UK;
- Entering into or 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 the 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 a prejudice and investigation.

3.3 Under section 18 of the Terrorism Act 2000 it is an offence for a person to enter into or become concerned in an arrangement which facilitates the retention of control by or on behalf of another person of terrorist property by concealment, removal from the jurisdiction, transfer to nominees or in any other way. Terrorist property is defined as money or other property which is likely to be used for the purposes of terrorism, proceeds of the commission of acts of terrorism, and proceeds of acts carried out for the purposes of terrorism.

3.4 Money laundering regulations apply to cash transactions in excess of €15,000 (approximately £13,000). However, POCA applies to all transactions and can include dealings with agents, third parties, property or equipment, cheques, cash or bank transfers.

3.5 Although instances of suspected money laundering are likely to be rare, given the nature of services provided by the Council, failure to comply with legal requirements could have significant implications for both the Council and the individuals concerned.

4 What are the Obligations on the Council ?

4.1 Whilst Local Authorities are not directly covered by the requirements of the MLR 2017, guidance from finance and legal professions, including the Chartered Institute of Public Finance and Accountancy (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.

4.2 The MLR 2017 applies to 'relevant persons' acting in the course of business carried out by them in the UK. Not all Local Authority business is 'relevant' for the purposes of the legislation. It is mainly the accountancy and audit services together with certain financial, company and property transactions carried out by legal services. However, the safest way to ensure compliance with the law is to apply it to all areas of work undertaken by the council, and ensure all individuals comply with the procedures set out in the policy. That way the Council will properly discharge its obligations under the money-laundering regime which is to:

- Appoint a Money Laundering Reporting Officer (MLRO) to receive disclosures from individuals of money-laundering activity;
- Implement a procedure to enable the reporting of suspicions of money laundering;
- Maintain client identification and record-keeping procedures in certain circumstances;
- Conduct money laundering risk assessments and adopt appropriate internal controls.

4.3 It is management's responsibility to implement systems of internal control capable of identifying unusual or suspicious transactions or customer activity and quickly report the details to the MLRO, as detailed in paragraph 5.1 below. Systems of internal control should include the following:

- Identification of senior management responsibilities;
- Provision of information to senior management on money-laundering and terrorist financing risks;
- Training of relevant employees on the legal and regulatory responsibilities for money-laundering and terrorist financing controls and measures;
- Documentation of the councils risk management policies and procedures.
- Measures to ensure that money-laundering and terrorist financing risks are taken into account in the day-to-day operations of the Council.

5 The Money Laundering Reporting Officer

5.1 The officer nominated to receive disclosures about money laundering/terrorist financing activity within the Council is the Director of Finance & Investment, who can be contacted as follows:

Director of Finance & Investment
Wallasey Town Hall
Brighton Street
Wallasey
Wirral
CH44 8ED

Telephone: 0151 691 8688
Email: aml@wirral.gov.uk

5.2 The Assistant Director of Finance & Investment is authorised to deputise in the absence of the MLRO.

6 Procedures

Cash payments

6.1 Usually for cash transactions, by way of custom and practice, banks, building societies and other financial institutions automatically report movement of over £1,000 to the National Crime Agency (NCA); so in order to avoid the Council being caught out by this reporting system and thus perceived to be at suspicion of assisting money laundering or terrorist financing, the Council has implemented a policy on the acceptance of cash. Identification will now be requested from all customers paying amounts over £1,000 in cash (See Appendix 2 - Verification of Customer Identity form. **Any** transactions that appear suspicious must be reported to the MLRO. (See Appendix 1 - Briefing Note for front line Employees, for a quick reference guide)

6.2 It's all about traceability. Consequently, cheques, large or small, coming in from UK clearing banks are easily traceable through the banking system, hence a shelf company paying a cheque to the Council for, say, £100,000 is traceable. An individual walking in with £1,005 cash to pay a debt is not necessarily traceable. Therefore best practice is to insist on payment by cheque or electronic transfer from a UK Clearing Bank: **NOTHING** overseas or offshore should be accepted.

7 Disclosure Procedure

Reporting to the Money Laundering Reporting Officer

7.1 Where an individual knows or suspects that money laundering or terrorist financing activity is taking/has taken place, or become concerned that their involvement in a matter may amount to a prohibited act under the legislation, they must disclose this as soon as practicable to the MLRO using the Money Laundering reporting form. The disclosure should be within "hours" of the information coming to your attention, rather than weeks or months later. **If a relevant matter is not disclosed immediately, then that individual may be liable to criminal prosecution.** Incidents MUST be reported in confidence and in private (See 7.4) – Individuals must NOT 'tip off' anybody else or allow anybody else to see or hear what is happening - it is CONFIDENTIAL between the reporting individual and the MLRO.

Reporting individuals may wish to consult with line managers before approaching the MLRO, however must be aware that **both the individual and the line manager** would have to disclose a report to the MLRO individually. This is because it is not a defence to presume that a report to the MLRO has been made on your behalf. If an individual does not consult with their line manager prior to making a report to the MLRO they **must not** discuss any aspect of the matter with their line manager or any other person without prior approval from the MLRO.

7.2 Reporting individuals must include as much detail as possible, for example:

- Full details of the people involved (including yourself, if relevant);
- Full details of the nature of their/your involvement;

If an individual has concerns that their involvement in the transaction would amount to a prohibited act, then the report must include all relevant details, as consent will be needed from the "NCA", via the MLRO, to take any further part in the transaction - this is the case even if the customer gives instructions for the matter to proceed before such consent is given.

  - Reporting individuals should therefore make it clear in the report if such consent is required and clarify whether there are any deadlines for giving such consent e.g. a completion date or court deadline;

- The types of money laundering activity involved:
  - If possible, cite the section number(s) under which the report is being made e.g. a principal money laundering offence under section 327 – 329 of the Act, or general reporting requirement under section 330 of the Act, or both (See Appendix 4, Offences Table);
- The dates of such activities, including:
  - Whether the transactions have happened, are ongoing or are imminent;
- Where they took place;
- How they were undertaken;
- The (likely) amount of money/assets involved;
- What form of documentation have been obtained to confirm identity;
- Why, exactly, they are suspicious – the NCA will require full reasons;

along with any other relevant available information to enable the MLRO to make a sound judgement as to whether there are reasonable grounds for knowledge or suspicion of money laundering and to enable them to prepare the report to the NCA, where appropriate.

7.3 Once the matter has been reported to the MLRO all directions provided must be followed. **No further enquiries should be made at this point**; any necessary investigation will be undertaken by the NCA. Suspicions should be reported to the MLRO who will refer the matter on to the NCA if appropriate. All Members, employees, partners, external bodies working on behalf of the Council will be required to co-operate with the MLRO and the Authorities during any subsequent money laundering/terrorist financing investigation.

7.4 Similarly, **at no time and under no circumstances should reporting individuals voice any suspicions** to the person(s) who is suspected of money laundering or terrorist financing, even if the NCA has given consent to a particular transaction proceeding, otherwise a criminal offence of "tipping off" may be committed.

7.5 Even saying "I can't tell you" may infer tip off. Advice may be sought from the MLRO if any uncertainty remains regarding how to proceed in such a situation. If and when the MLRO and/or the NCA give clearance individuals must proceed with the matter as if nothing had happened.

7.6 The MLR 2017 creates a new criminal offence in that any person who recklessly makes a statement in the context of money-laundering which is false or misleading commits an offence. Punishment is a fine and/or up to 2 years' imprisonment.

7.7 Reporting individuals should not therefore, make any reference on a client file to a report having been made to the MLRO – should the client exercise their right to see the file, then such a note would obviously tip them off to the report having been made. The MLRO will keep the appropriate records in a confidential manner.

Consideration of the Disclosure by the Money Laundering Reporting Officer

7.8 Upon receipt of a disclosure report, the MLRO must note the date of receipt on their section of the report and acknowledge receipt of it. They should also advise you of the timescale within which they expect to respond to you.

7.9 The MLRO 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;
- Any identification evidence held.

and undertake such other reasonable enquiries they think appropriate in order to ensure that all available information is taken into account in deciding whether a report to the NCA is required (enquiries being made in such a way as to avoid any appearance of tipping off those involved). The MLRO may also need to discuss the report with you.

7.10 Once the MLRO 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/terrorist financing taking place; or
- There are reasonable grounds to know or suspect that is the case; and
- Whether they need to seek consent from the NCA for a particular transaction to proceed.

7.11 Where the MLRO does so conclude, then they must disclose the matter as soon as practicable to the NCA on their **standard report form** and in the prescribed manner, unless they have a reasonable excuse for non-disclosure to the NCA (for example, if you are a lawyer and you wish to claim legal professional privilege for not disclosing the information). Up to date forms can be downloaded from the NCA website at www.nationalcrimeagency.gov.uk.

- Where the MLRO considers no money laundering/terrorist financing is taking place or suspects money laundering or terrorist financing but has a reasonable excuse for non-disclosure, then they must note the report accordingly; they can then immediately give their consent for any ongoing or imminent transactions to proceed. Remember - it's better to disclose than not – "better safe than sorry".
- In cases where legal professional privilege may apply, the MLRO must liaise with the Director of Governance and Assurance to decide whether there is a reasonable excuse for not reporting the matter to the NCA.
- Where consent is required from the NCA for a transaction to proceed, the transaction(s) in question must not be undertaken or completed or proceed until the NCA has specifically given consent, or there is deemed consent through the expiration of the relevant time limits without objection from the NCA.

7.12 Where the MLRO concludes that there are no reasonable grounds to suspect money laundering/terrorist financing then they shall mark the report accordingly and give their consent for any ongoing or imminent transaction(s) to proceed.

7.13 All disclosure reports referred to the MLRO and reports made by them to the NCA must be retained by the MLRO in a confidential file kept for that purpose, for at least 5 years from the end of the business relationship.

7.14 The MLRO commits 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/terrorist financing and they do not disclose this as soon as practicable to the NCA.

8 Due Diligence Requirements

8.1 Where the Council is carrying out certain 'regulated activity' [1] then extra care needs to be taken to check the identity of the customer or client and understand their business. This is known as carrying out Customer Due Diligence (CDD). (See Appendix 3 for CDD procedure and Sources of Evidence document). This is necessary so that the Council is in a position to know if there is suspicious activity that should be reported; clearly it is only by the Council knowing its clients and their businesses that it can recognise abnormal and possibly suspicious activity.

8.2 CDD must be carried out when the Council is undertaking regulated activities, and:

- Intends to establish a business relationship;
- Is carrying out an occasional transaction that amounts to a transfer[2] of funds exceeding €1,000;
- Is carrying out an occasional transaction that amounts to €15,000 or more, whether or not it is executed in a single operation or in several operations which appear to be linked;
- Money laundering or terrorist financing is suspected;
- There is doubt over the veracity or adequacy of documents or information previously obtained the purposes of identification or verification.

8.3 CDD should be applied on a risk sensitive basis for existing customers and must be carried out during the life of a business relationship, but should be proportionate to the risk of money laundering and terrorist funding, based on the officer's knowledge of the customer and a regular scrutiny of the transactions involved.

8.4 Where there is a beneficial owner who is not the customer, then the Council must take reasonable measures to verify their identity and where the beneficial owner is a trust or similar, then the Council must understand the nature of the control structure of that trust.

8.5 If satisfactory evidence of identity is not obtained at the outset then the business relationship or one off transaction cannot proceed any further.

8.6 Under MLR 2017, simplified due diligence is only permitted where it is determined that the business relationship or transaction presents a low risk of money laundering or terrorist funding, taking into account the Council's assessment of the risk.

8.7 Enhanced due diligence must be undertaken in addition to CDD, on a risk sensitive basis, in the following circumstances:

- When the customer is not physically present when identification checks are undertaken;
- When business relationships are entered into 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;
- When you enter into a transaction with a person from a high risk third country identified by the EU ;
- Any other situation where there's a higher risk of money laundering or terrorist financing.

8.8 Enhanced due diligence should include obtaining any additional documentation, data or information that will confirm the customer's identity and/or the source of the funds to be used in the business relationship/transaction.

8.9 If, at any time, it is suspected that a client or customer for whom the Council is currently, or is planning to carry out a regulated activity is carrying out money laundering or terrorist financing, or has lied about their identity, then this must be reported to the MLRO.

---

[1] Regulated activity is defined as the provision 'by way of business' of: advice about tax affairs; accounting services; treasury management, investment or other financial services; audit services; legal services; estate agency; services involving the formation, operation or arrangement of a company or trust or; dealing in goods wherever a transaction involves a cash payment of €15,000 or more.

[2] Any transaction at least partially carried out by electronic means on behalf of a payer through a payment service provider, with a view to making funds available to a payee through a payment service provider, irrespective of whether the payer and the payee are the same person and irrespective of whether the payment service provider of the payer and that of the payee are one and the same.

9 Guidance and Training

9.1 In support of the Policy and Procedures, the Council will:

- Make all Members, employees, partners, external bodies working on behalf of the Council aware of the requirements and obligations placed on the Council and on themselves as individuals by the 2017 MLRs; and
- Give targeted training to those most likely to encounter money laundering/terrorist financing, as identified in the risk assessment.

10 Conclusion

10.1 The legislative requirements concerning anti-money laundering procedures are lengthy and complex. This Policy has been written to enable the Council to meet the legal requirements in a way which is proportionate to the risk to the Council of contravening the legislation.

10.2 If individuals have any concerns whatsoever regarding any transactions then they should contact the MLRO.

11 Monitoring and Review of Compliance

11.1 It is the responsibility of all Chief Officers to undertake regular monitoring and review of their department's compliance with the Anti-Money Laundering Policy and Procedure and in particular to ensure that the procedure to be adopted is communicated to all Members, employees, partners, external bodies working on behalf of the Council.

12 Record Keeping

12.1 Copies of documents and information used to fulfil CDD obligations must only be processed for the purposes for which they are intended and should be kept for a period of 5 years following the completion of a transaction or the end of business relationship. At the end of the 5 year period personal data should be deleted unless:

- The Council is required to retain records containing personal data under an enactment or for the purposes of court proceedings, or there are reasonable grounds for believing the records need to be retained for legal proceedings, or;
- The Council has the consent of the person whose data it is.

13 Policy Review

13.1 The Policy will be reviewed on an annual basis and updated/amended when new legislation/guidance is issued, to ensure all information is accurate and up-to-date.

Document Ownership	
Policy owned by:	Mark Niblock, Chief Internal Auditor, Internal Audit – Business Services
Policy documented by:	Luan Quirke, Lead Auditor, Internal Audit
Date policy documented:	July 2018
Date policy due for 1st review:	July 2019

Version Control Table

All changes to this document are recorded in this table

Date	Notes/Amendments	Officer	Next Scheduled Review Date