ANTI-MONEY LAUNDERING POLICY & FRAMEWORK

1.0 INTRODUCTION

1.1 The Policy is written in order for the Council to meet its obligations under the UK's Proceeds of Crime Act 2002 (POCA) and the Money Laundering Regulations 2007 (the Regulations).

1.2 It is adopted under Part 4 of the Council's Constitution and specifically in order to help prevent fraud and corruption under Financial Procedure Rules (Section C).

Policy Statement

1.3 The Council will do all it can to:

- Prevent, wherever possible, the organisation, its employees and Members being exposed to money laundering. This includes temporary and agency staff, the Council's contractors and partners.

- Identify the potential areas where money laundering may occur and take appropriate action to minimise the risk.

- Comply with all legal and regulatory requirements, especially with regard to the reporting of actual or suspected cases.

1.4 However, as a public authority, every employee and Member also has a personal responsibility to be vigilant.

2.0 SCOPE OF THE POLICY

2.1. The Policy applies to all members and employees of the Council and aims to maintain the high standards of conduct that currently exist within the Council by preventing criminal activity through money laundering. The Policy sets out the procedures that must be followed (for example reporting suspicions of money laundering activity) to enable the Council to comply with its legal obligations.

2.2 This Policy is designed to alert employees to the risk of the Council receiving sums of money in circumstances that give rise to suspicion and /or knowledge of money laundering.

2.3. Anti money laundering legislation places responsibility upon all Council employees to prevent money laundering. This covers a wide area of financial transactions, including possessing, or in any way dealing with, or concealing, the proceeds of any crime.

2.4. Specifically, it applies to all employees involved with cash transactions either on a regular or ad-hoc basis.

2.5. In addition, under the Proceeds of Crime Act (POCA) 2002, where the Council is carrying out what is termed "**relevant business,**" regulations require that satisfactory due diligence is undertaken before any transaction is undertaken.

2.6. In this case, relevant business includes:

- Accountancy
- Audit
- Taxation
- Other Financial Services such as Treasury Management
- Legal Services

2.7. The legislation puts a personal responsibility on all individuals to report suspicions of money laundering. It is a criminal offence to:

- Assist a money launderer.
- "Tip off" a person suspected to be involved in money laundering that they are suspected or that they are the subject of police investigations.
- Fail to report a suspicion of money laundering.
- Acquire, use or possess criminal property.

2.8 Contravening the legislation could lead to a fine or even imprisonment. Formal action in line with the Council's Disciplinary Procedure would also be taken against any Member or employee suspected of contravening the terms of this Policy.

3.0 WHAT IS MONEY LAUNDERING

3.1 Money laundering is any activity used to conceal/disguise the nature, source, location, ownership or control of currency (or assets). It is most often an attempt to hide the proceeds of dishonest or criminal activity and to try to give the impression that the income is from a legitimate source so that it can be used.

3.2 It is often associated with large scale crime such as drug trafficking, terrorist funding and financial crimes involving fraud. UK legislation also applies to any level of activity used to conceal the source of income to the benefit of an individual.

3.3 This can be anything from the proceeds of petty theft or from hiding income to commit benefit fraud, up to larger corporate crimes which can involve complex and well planned linked transactions.

The Council's Risk

3.4 The Council is at risk of being used in money laundering activity as many of its transactions could appear attractive to someone looking to launder money. For example, the Council collects large sources of income including housing rents, business rates and council tax, which could provide channels to use laundered money.

3.5 In addition, overpayments could be deliberately made and then a refund requested. This would generate a payment from the Council and provide a legitimate source for the income.

3.6 Other areas at risk include property deals, including right to buy transactions, regeneration/development schemes, partnerships with private sector firms and treasury management activities.

4.0 PURPOSE OF THE POLICY

4.1 The overall legislative requirements concerning anti-money laundering procedures are extensive and complex. This Policy has been written so as to enable the Council to meet the legal requirements in a way that is proportionate to the Council contravening this legislation.

4.2 The object of this Policy is to make all employees aware of the legislative requirements and their role in relation to this Policy.

4.3 Potentially, any employee or Member could be caught by the money laundering provisions, if they suspect money laundering and either become involved with it in some way and/or do nothing about it.

4.4 Whilst the risk to the Council of contravening the legislation is considered low, it is extremely important that all Members and employees are familiar with the legal requirements.

4.5 This framework aims to provide all employees and members with a structured, supported process by which they can raise concerns of money laundering and to provide information on how they could be affected by the legislation.

5.0 MONEY LAUNDERING REQUIREMENTS

5.1 To meet the requirements of the Council, these are:

- Provision of training to relevant Members and employees on the requirements of the legislation, including the identification of suspicious transactions, identity verification and reporting procedures.

- Designation of an officer as the Money Laundering Reporting Officer (MLRO) who will receive any report, keep records and if considered

appropriate, make reports to the National Criminal Intelligence Service (NCIS).

- Establishment of procedures for employees to report any suspicions to the Council's nominated MLRO.

6.0 TRIGGER POINTS

6.1 Under the Policy, employees dealing with money transactions will be required to comply with certain procedures. These procedures apply in the circumstances set out below:

Monetary Receipts

6.2 A substantial amount of transactions are undertaken electronically via direct debit, BACS and from debit/credit card. However, the Council receives money at the Civic Offices and Etwall Leisure Centre, together with ad-hoc payments that are taken for fees and charges at the point of service delivery.

6.3 Although there are still a large number of transactions, individual values are relatively small, whereas money laundering tends to involve larger amounts of currency.

6.4 Based on this, the procedures in this Policy apply whenever a cash payment is received for **£2,000 or more**, this being the limit generally recommended in the Regulations.

Relevant Business

6.5 Where the Council is carrying out relevant business (as defined in Section 2.6, above) and forms an ongoing business relationship with a client, the procedures in this Policy apply:

- Each time a one-off transaction is made by or to the client of 15,000 Euro (approximately £12,750) or more.

- Where a series of linked one-off transactions involving a total payment by or to the client of 15,000 Euro (approximately £12,750) or more.

- When it is known or suspected that a one-off transaction (or a series of them) involves money laundering or terrorist financing.

Note – the trigger point of 15,000 Euro is in accordance with the European Union 3rd Money Laundering Directive which has been incorporated into UK legislation.

7.0 CLIENT IDENTIFICATION PROCEDURE

7.1. Where a trigger point is reached, any employee involved in one or more of the associated transactions should ensure the client provides satisfactory evidence of their identity. This applies to existing clients as well as new ones.

7.2. This should be done in person by the client, through passport and or driving licence that also incorporates a **photograph**, plus one other document with their **name and address**. These documents must be one of the following

- Gas, Water or Electricity Bill
- Telephone Bill (but not a Mobile)
- Mortgage Statement
- Bank or Building Society Book
- Pension Book

7.3. In the case of a company, partnership or sole trader, etc. corporate identity should be obtained. This should be through company formation documents with a company registration number where appropriate, together with a business rate demand notice.

7.4. Clearly, monetary transactions or relevant business which breach the trigger points may well be legitimate.

7.5. **However, it is important in these circumstances that the employee only explains to the client that they are acting in accordance with the Council's Financial Procedural Rules if they are challenged when asking to provide evidence. To avoid a possible "tipping off" scenario, they should say no more or they may be committing a criminal offence**.

7.6. In circumstances where the client cannot be physically identified the employee should be aware that there is greater potential for money laundering where they are not physically present. If the client acts, or appears to act for another person, reasonable measures must be taken for the purposes of identifying that person.

7.7. This should include authorisation from the person concerned or from other legal title that the client is acting for another person. The client should also be asked for identification as set out in 7.1 and 7.2 above.

7.8. **If satisfactory evidence is not obtained the relationship or the transaction should not proceed**.

8.0 CUSTOMER DUE DILIGENCE PROCEDURE

8.1 Customer Due Diligence (CDD) is a procedure which is carried out when undertaking relevant business. To meet the POCA regulations, this requires that extra care is taken to check the identity of the client.

8.2 This need not be onerous, especially where the client is known to the Council and some simple and quick checks can be made. Firstly, the following questions should be asked to determine whether CDD is relevant:

- Is the service being provided a regulated activity?
- Is the Council charging for the service?
- Is the service being provided to a customer other than a UK public authority?

8.3 If the answer to **any** of the above questions is **no** then it is not necessary to carry out any further CDD. If the answer to **all** these questions is **yes** it is then necessary to undertake CDD before any business relationship can commence with the customer. If there is any uncertainty whether CDD is required, the MLRO should be contacted for advice.

8.4 CDD should be proportionate and its purpose is to verify that the customer is who they say they are and that their money comes from a legitimate source, is being used for a legitimate purpose and that the transaction taking place is legitimate.

8.5 CDD can be achieved by conducting some simple enquiries such as:

- Checking with the Customer's web-site to confirm their business address.

- Conducting a credit/company check through Companies House to confirm the nature of their business, trading position, VAT status and the identity of the directors (**this query should be referred to the Council's Internal Audit Unit**).

8.6 It is a requirement under CDD that it applies as soon as the Council becomes involved with a new customer. CDD is an ongoing process and it should also be applied on a proportionate basis for existing customers taking into account the risk of money laundering and terrorist funding.

8.7 Where doubt exists, enhanced CDD may be required where additional evidence should be gathered. In particular, this will be relevant where:

- The Customer's appointed representative has not been physically present for identification.

- The customer is a politically exposed person; that is an individual who at any time in the previous year has held a prominent public function outside of the UK and EU or international institution/body, this also includes their immediate family members or close associates.

- There is a beneficial owner who is not the direct client. A beneficial owner is a person who holds more than 25% of the shares, voting rights or interest in a company, partnership or trust.

8.8 To satisfy the requirements of enhanced CDD, additional documentation, data or information confirming the client's identity and/or the source of the finances to be used in the business relationship or transaction should be obtained.

8.9 **If it becomes necessary to engage in enhanced CDD, the MLRO must be notified prior to undertaking any action**.

Record Keeping Procedure

8.10 Details of all relevant business transactions, including client identification evidence must be maintained for at least **five years** from the completion of the transaction. Details may be required as evidence in any subsequent investigation by the authorities into money laundering.

8.11 The precise nature of the records is not prescribed by law. However, they must provide an audit trail that can be used during any subsequent investigation. This should include details of the client and the relevant transaction, together with a record of what form funds were received or paid.

9.0 THE MONEY LAUNDERING REPORTING OFFICER (MLRO)

9.1 The Officer nominated to answer queries and to receive disclosures about money laundering activity within the Council is the Section 151 (Chief Finance Officer) which is the Director of Corporate Services. In their absence, the nominated Deputy is the Head of Finance and Property Services.

9.2 The MLRO will utilise the services of Internal Audit, the Council's Monitoring Officer and the Internal Fraud Investigation Unit, where this is considered necessary.

10.0 INTERNAL REPORTING PROCEDURE

10.1 Where an employee takes a payment or enters into relevant business where the trigger points have been breached but the associated transactions meet the identification and CDD requirements as set out in this Policy, i.e. they are deemed legitimate, then details should be recorded on the form in **Appendix 1**. **The form should be completed immediately after the transaction has taken place and passed directly by the employee to the MLRO.**

10.2 In addition, where an employee is aware that money laundering may have taken place or may be taking place they must immediately contact the MLRO for guidance regardless of the amount involved. In such circumstances, no money must be taken or a transaction entered into until this has been done.

10.3 Any employee knowing or suspecting money laundering, fraud or the use of the proceeds of crime must also report this to the MLRO on the Form in **Appendix 2**. **Again**, **the form should be completed immediately a suspicion arises and passed directly by the employee to the MLRO.**

10.4 Examples of how money laundering could take place, together with possible warning signs to observe, are set out in **Appendix 3**.

10.5 Upon receiving a report, the MLRO will consider all of the admissible information in order to determine whether there are grounds to suspect money laundering.

10.6 If the MLRO determines that the information or matter should be disclosed it will be reported to the National Criminal Intelligence Service (NCIS).

Reporting to the NCIS

10.7 Disclosure to the NCIS must be as soon as practicable on their standard report form and in the prescribed manner unless there is a reasonable excuse for non-disclosure. Where consent is required from the NCIS for a transaction to proceed, then the transaction(s) in question must not be undertaken or completed until the NCIS has specifically given consent, or there is deemed consent through the expiration of the relevant time limits without objection from the NCIS.

10.8 Where the MLRO suspects money laundering but has reasonable excuse for non-disclosure, the report must be recorded and consent given for any ongoing transactions to proceed. Where there are no reasonable grounds to suspect money laundering, the report will be marked accordingly and consent given for any ongoing transactions to proceed.

10.9 Once the details have been referred to the MLRO, employees must follow their directions, but must not make additional enquiries into the matter themselves. Employees will be required to co-operate with the MLRO and investigating authorities where required.

10.10 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 and they do not disclose this as soon as practicable to the NCIS.

Tipping Off

10.11 During this process the client must not be tipped off. **At no time and under no circumstances should an employee voice any suspicions** to the person(s) suspected of money laundering, even if the NCIS has given consent to a particular transaction proceeding, otherwise the employee may be committing a criminal offence of “tipping off.”

10.12 Therefore, no reference should be made on a client file to a report having been made to the MLRO. Should the client exercise their right to see a file, then such a note will obviously tip them off to the report having been made and may render the employee liable to prosecution. The MLRO will keep the appropriate records in a confidential manner.

11.0 OTHER PROCEDURES

Regular Receipts

11.1 The Council in the normal operation of its services accepts many payments from individuals and organisations. For all transactions under £2,000 the Money Laundering regulations do not apply.

11.2 However, employees should be aware of regular cash payments and if there are reasonable grounds to suspect money laundering activities, proceeds of crime or is even simply suspicious, the matter should still be reported to the MLRO on the relevant form in **Appendix 2**.

Refunds

11.3 Care should be taken when dealing with refunds. For example, a significant overpayment which results in a repayment will need to be properly investigated and authorised before payment.

11.4 In the event of any suspicious transactions, the MLRO must be contacted immediately to investigate the case.

11.5 As highlighted elsewhere in the Policy, the client should not be informed and consequently “tipped off.”

Training

11.6 The Council will take appropriate measures to ensure that all Members and employees are made aware of the regulations and the existence of this Policy, together with their roles and responsibilities.

11.7 Staff that are more likely to be involved in monetary payments and in relevant business as defined by the regulations are given specific training in how to recognise and deal with transactions that may be related to money laundering.

11.8 This mainly applies to employees in Finance, Customer Services, Legal and Housing, together with anyone else nominated by a Head of Service.

APPENDIX 1

RECORD OF A TRANSACTION THAT BREACHES A TRIGGER POINT

Date of Transaction;

Officer Reporting:

Position:

Contact Details:

CLIENT DETAILS

Name and Title:

Address:

Company Number (If relevant):

Type of Business:

Evidence Seen and Verified:

NATURE OF TRANSACTION

Amount:

Purpose:

Any Other Details:

RECEIPT FROM MLRO

Reference:

Date:

Signature:

APPENDIX 2

DISCLOSURE FORM TO MLRO

Date of disclosure:

Member/Officer making disclosure:

Position:

Contact Details:

CLIENT DETAILS

Name and Title:

Address:

Company Number (If relevant):

Type of Business:

Any Other References or Details:

REASON FOR DISCLOSURE

This should indicate the suspected or known activity with supporting details and evidence.

RECEIPT FROM MLRO

Reference:

Date:

Signature:

APPENDIX 3

Money Laundering - Warning Signs

The following examples could indicate that money laundering is taking place:

1. Transactions or trade that appear to make no commercial or economic sense from the perspective of the other party

A money launderer's objective is to disguise the origin of criminal funds and not necessarily to make a profit. A launderer may therefore enter into transactions at a financial loss if it will assist in disguising the source of the funds and allow the funds to enter the financial system.

2. Large volume/large cash transactions

All large cash payments should be the subject of extra care and before accepting cash the reasons for such payments should be fully understood. Payments should be encouraged through the banking system to avoid problems.

3. Payments received from third parties

Money launderers will often look to legitimate business activity in order to assist in 'cleaning' criminal funds and making payments on behalf of a legitimate company can be attractive to both parties. For the legitimate company it can be a useful source of funding and for the launderer the funds can be repaid through a banking system.

4 Warning signs of organised money laundering

- Use of cash where other means of payment are normal
- Unusual transactions or ways of conducting business
- Unwillingness to answer questions/secretiveness generally
- Use of overseas companies
- New companies
- Overpayments of Council Tax where refunds are needed