Buckinghamshire Council

Anti-Money Laundering Policy

A guide to the Council's anti-money laundering safeguard and reporting arrangements.

Prepared by: Maggie Gibb, Head of Business Assurance (& Chief Internal Auditor)

Version 1.5– June 2021

Version	Date	Sign Off	Action	Responsible Officer
1.0	14/11/2019	Resources Board	Agreed. Minor changes to reflect structures	Maggie Gibb
1.1	26/11/2019	Chief Executive's Implementation Group	Agreed. Minor changes to reflect structures	Maggie Gibb
1.2	11/12/2019	Informal Shadow Exec	Agreed.	Maggie Gibb
1.3	01/06/2021	Head of Business Assurance (& Chief Auditor)	Agreed. Minor changes	Maggie Gibb
1.4	14/06/2021	Audit Board	Agreed.	Maggie Gibb
1.5	22/06/2021	Audit & Governance Committee		

Anti-Money Laundering Policy

1. Introduction....1
2. Scope of the policy....2
3. What is money laundering?....3
4. What are the obligations on the council?....4
5. The importance of disclosing any suspicions to the Money Laundering Reporting Officer (MLRO)....5
6. Customer Due Diligence....7
7. Enhanced Customer Due Diligence and Ongoing Monitoring....8
8. Internal Clients....9
10. Record Keeping....10
11. Money Laundering Reporting Officer....10

APPENDIX 1 Customer Due Diligence Pro-Forma....101

1. Introduction

1.1. On 10 January 2020 changes to the Government's Money Laundering Regulations (MLRs) came into force. The changes update the UK's Anti Money Laundering regime to incorporate international standards set by the Financial Action Task Force (FATF). The 2019 Regulations amend**:**

- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs).

1.2. As an overview, the changes incorporate the requirement to keep an up to date list of exact functions that qualify as prominent public functions, the requirement on enhanced due diligence when working with high risk countries, the requirement to maintain registers of beneficial owners, a reduced limit of pre-paid cards and electronic money, enhanced due diligence on virtual currencies/crypto currencies/digital tokens and letting agency activities to be brought within the scope of Anti-Money Laundering.

1.3. A key difference is the 5th Money Laundering Directive brings additional businesses into the scope of the anti-money laundering regulatory framework. Described as "obliged entities" in the 4th Money Laundering Directive, these are defined as "relevant persons" in the MLRs and as businesses in the "regulated sector" in the Terrorism Act 2000 and the Proceeds of Crime Act 2002. The requirements of the 5th Money Laundering Directive do not allow for the exemption of small businesses or any exemptions based on size.

1.4. In identifying ownership, the 2019 Regulations introduces an explicit Customer Due Diligence (CDD) requirement for relevant persons to take reasonable measures to understand the ownership and control structure of their customers. Relevant persons must also take reasonable measures to verify the identity of senior managing officials when the beneficial owner of a body corporate cannot be identified.

1.5. Although Anti-Money Laundering legislation does not specifically cover local authorities as defined by organisations in the regulatory sector, it is implied best practice that we assess the risk and put sufficient controls in place to prevent the Council from being used for money laundering.

1.6. We are also required to:

- assess the risk of Buckinghamshire Council being used by criminals to launder money;
- check the identity of our customers;
- check the identity of 'beneficial owners' of corporate bodies and partnerships;
- monitor our customers' business activities and report anything suspicious to the National Crime Agency (NCA);
- make sure we have the necessary management control systems in place; keep all documents that relate to financial transactions, the identity of our customers, risk assessment and management procedures and processes;

- make sure our employees are aware of the regulations and have had the necessary training; and
- relevant persons must have policies to ensure they undertake risk assessments prior to the launch or use of new products or business practices, as well as new technologies.

2. Scope of the policy

2.1 This Policy applies to all employees whether permanent or temporary and Members of the Council. Its aim is to enable employees and Members to respond to a concern they have in the course of their dealings for the Council. Individuals who have a concern relating to a matter outside of work should contact the Police.

2.2 Failure by a member of staff to comply with the procedures set out in the Policy should be escalated for appropriate action to be taken.

3. What is money laundering?

3.1 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; and/or
- 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.

3.2 Money laundering activity may range from a single act, for example being in possession of the proceeds of one's own crime, to complex and 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 clients, their counterparties and others laundering money in any of its many forms.

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 or 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 (including any resources of a prescribed organisation), proceeds of the commission of acts of terrorism, and proceeds of acts carried out for the purposes of terrorism.

3.4 It is important to note that anyone, Council employee or not, can commit any of the above offences. However, in addition to these offences there are a series of obligations imposed on the Council by the 2007 Money Laundering Regulations that it must fulfil, and of which breach can also amount to an offence by the Council.

4. What are the obligations on the council?

4.1 Whilst Local Authorities are not directly covered by the requirements of the Money Laundering Regulations 2019, 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.

4.2 The regulations apply to "relevant persons" acting in the course of business carried out by them in the UK. Relevant persons must check beneficial ownership registers of legal entities in scope of the People with Significant Control (PSC) requirements before establishing a business relationship. Where there is a discrepancy between the beneficial ownership information on the registers and the information that is made available to them in the course of carrying out CDD, there is a requirement to report these discrepancies to Companies House. Companies House will investigate and, if necessary, resolve the discrepancy in a timely manner. These reports are excluded from public inspection. Not all of the Council's business is relevant for the purposes of the Regulations; it could include accountancy and audit services carried out by Financial Services and the financial, company and property transactions undertaken by Legal Services.

4.3 It is reasonable to conclude that the money laundering regime is not primarily aimed at local authorities and that local authorities' work is to some extent tangential to the regime. However, the safest way to ensure compliance with the regime is nonetheless to apply its requirements to all of the Council's areas of work and to ensure that all staff comply with the reporting procedure set out in the Policy.

4.4 The obligations on the Council are to establish and maintain appropriate and risk-sensitive policies and procedures relating to the following:

- customer due diligence measures and ongoing monitoring;
- reporting;
- record-keeping;
- internal control;
- risk assessment and management;
- the monitoring and management of compliance with, and the internal communication of such policies and procedures.

4.5 All employees are required to follow the procedure set out in the Policy and in this way the Council will properly discharge its obligations under the money laundering regime.

5. The importance of disclosing any suspicions to the Money Laundering Reporting Officer (MLRO)

5.1 Where you know or suspect that money laundering activity is taking/has taken place, or you are concerned that your involvement in the matter may amount to a prohibited act under the legislation, you must disclose to the MLRO this suspicion or concern as soon as practicable. The disclosure should be made within hours rather than days or weeks of the information coming to your attention. The legislation determines that a single cash transaction or a series of linked transactions totalling over €15,000 (approximately £13,000 at the time of the legislation) should be treated as suspicious. However, vigilance also needs to be maintained in respect of all other possibilities such as a series of smaller payments in cash.

IF YOU FAIL TO DO SO YOU MAY BE LIABLE TO PROSECUTION.

5.2 Your disclosure should be made to the MLRO on the Pro-Forma attached. The report must include as much detail as possible, for example:

- full details of the people involved (including yourself if relevant) e.g. name, date of birth, address, company names, directorships, phone numbers etc.;
- if you are concerned that your involvement in the transaction would amount to a prohibited act under sections 327-329 of the 2002 Proceeds of Crime Act then your report must include all relevant details;
- you will need consent from the National Crime Agency (NCA) or relevant successor body, through the MLRO, to take any further part in the transaction. This is the case even if the client gives instructions for the matter to proceed before such consent is given. You 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;
- the date of such activities, including whether the transactions have happened, are on-going or are imminent;
- where they took place;
- how they were undertaken;
- the (likely) amount of money/assets involved;
- why, exactly, you are suspicious;
- in addition, any other information to enable the MLRO to make a sound judgment as to whether there are reasonable grounds for knowledge or suspicion of money laundering; and
- to prepare a report to the NCA, where appropriate. You should also enclose any copies of relevant supporting documentation.

5.3 As soon as you have reported the matter to the MLRO you must follow any directions they give to you. **You must NOT make any further enquiries into the matter yourself.**

Any necessary investigation will be undertaken by the NCA or relevant successor body as appropriate. All members of staff will be required to co-operate with the MLRO and the authorities during any subsequent money laundering investigation.

5.4 Similarly, **at no time and under no circumstances should you voice any suspicions** to the person(s)/organisation you suspect of money laundering, otherwise you may commit the criminal offence of "tipping off".

5.5 Do not, therefore, make any reference on a client file to a report having been made to the MLRO. Should the client exercise his/her right to see the file then such a note would obviously tip them off to the report having been made. Again you would be at risk of prosecution for tipping off. The MLRO will keep the appropriate records in a confidential manner.

6. Customer Due Diligence

6.1 Customer due diligence means that the Council must know its clients and understand their businesses. This is 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.

6.2 The obligations imposed on the Council must, of course, be brought into effect by its individual employees. Employees must therefore be familiar with these obligations.

6.3 The 2017 Regulations and 2019 (as amended) require that the Council identifies its customers and verifies that identity based on documents, data or information obtained from a reliable source. Where there is a beneficial owner who is not the customer then the Council must identify that person and verify the 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.

6.4 The Council must obtain information on the purpose and intended nature of the business relationship. The MLR 2019 introduces the need for the Council to consider both customer and geographical risk factors in deciding what due diligence is appropriate. The new Regulations introduced a list of high-risk jurisdictions which if involved in a transaction makes enhanced due diligence and additional risk assessment compulsory. On 13 February 2019, the European Commission updated its list of high-risk third countries under the European Union's Fourth Anti-Money Laundering Directive The list of areas is currently: Afghanistan, America Samoa, The Bahamas, Botswana, Democratic People's Republic of Korea, Ethiopia, Ghana, Guam, Iran, Iraq, Libya, Nigeria, Pakistan, Panama, Puerto Rico, Samoa, Kingdom of Saudi Arabia, Sri Lanka, Syiria, Trinidad and Tobago, Tunisia, US Virgin Islands, and Yemen. For an up to date list of such jurisdictions an officer should seek advice from the MLRO.

6.5 The checks described in the paragraph 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.

6.6 The Council is also obliged to maintain ongoing monitoring of its business relationships which means it must scrutinise transactions throughout the course of the relationship to ensure that the transactions are consistent with the Council's knowledge of the customer and keep the information about the customer up-to-date.

6.7 Where property transactions are carried out using externally appointed agents on behalf of the Council, the agent will be required to perform and evidence the "know your client checks (KYC)" and these should be shared and retained by the Council.

6.8 Where the Council is not able to apply the customer due diligence measures set out above it must not carry out a transaction with or for a customer through a bank account, it must not establish a business relationship or carry out an occasional transaction with the customer, it must terminate any business relationship with the customer and consider whether to make a disclosure.

6.9 However, the above paragraph does not apply where a lawyer or other professional adviser is in the course of advising the legal position for his/her client or performing his/her task of defending or representing that client in, or concerning, legal proceedings including the advice on the institution or avoidance of proceedings.

7. Enhanced Customer Due Diligence and Ongoing Monitoring

7.1 It will in certain circumstances be necessary to undertake what is known in the Regulations as Enhanced Customer Due Diligence. In summary, this will be necessary where:

- the customer has not been physically present for identification purposes; or
- in any other situation which by its nature can present a higher risk of money laundering or terrorist financing.

7.2 Where this applies, the Council will need to take adequate measures to compensate for the higher risk. For example, this will mean ensuring that the customer's identity is established by additional documents, data or information.

7.3 Similarly, where the Council is in an ongoing "business relationship" with a customer, the Regulations impose a special obligation to carry out ongoing monitoring. This means that the Council must:

- scrutinise transactions undertaken throughout the course of the relationship to make sure that these transactions are consistent with the Council's knowledge of the customer, his/her business and risk profile; and
- keep documents, data or information obtained for the purpose of applying Customer Due Diligence measures up-to-date.

7.4 The regulations require that enhanced customer due diligence measures are taken to manage and mitigate the risks exposed by politically exposed persons (PEPs). The term PEPs refers to people who hold high public office. The Council is required to have appropriate risk-management systems and procedures to identify when the customer is a PEP and to manage the enhanced risks arising from having a relationship with that customer. Business relationships with the family and known close associates of a PEP are also subject to greater scrutiny.

8. Internal Clients

8.1 Appropriate evidence of identity for Council departments will be signed, written instructions on Council headed notepaper or an e-mail on the internal system at the outset of a particular matter. Such correspondence should then be placed on the Council's client file along with a prominent note explaining which correspondence constitutes the evidence and where it is located.

9. External Clients

9.1 The MLRO will maintain a central file of general client identification and verification information about the Council's external clients to whom the Council provides professional services. You should check with the MLRO that the organisation or individual in respect of which you require identification and verification information is included in the MLRO's central file and then check the details of the information held in respect of the particular client. If the organisation or individual is not included in the central file you should discuss the matter with the MLRO.

9.2 In practice the Council can fulfil its obligations if employees complete the Customer Due Diligence Pro-Forma attached.

10. Record Keeping

10.1 The information gathered by the Council in pursuance of its customers due diligence obligations and described above must be kept for a period of five years from either the completion of the transaction or the end of the business relationship. Each Department or Section of the Council should nominate an officer who is to be responsible for the secure storage of these records.

11. Money Laundering Reporting Officer

11.1 The officer nominated to receive disclosure about money laundering activity within the Council is the Service Director - Corporate Finance (S151 Officer), who can be contacted as follows:

Service Director - Corporate Finance (S.151 Officer)
Buckinghamshire Council
The Gateway
Aylesbury
Buckinghamshire
HP20 1UA
01296 383120

In the absence of the MLRO the Monitoring Officer, the Corporate Director of Resources, is authorised to deputise.

They can be contacted at thee above address or on telephone 01296 303986.

APPENDIX 1

Customer Due Diligence Pro-Forma

SECTION A: PRELIMINARY	
NAME OF CUSTOMER	
Is this customer another public authority (E.g. a local authority)?	**If "Yes", the due diligence measures below in Sections B and C do not need to be applied.**
Does the Council suspect the customer of money laundering or terrorist financing?	**If "Yes", the suspicion MUST always be reported to the MLRO immediately.**

SECTION B: DUE DILIGENCE MEASURES

These measures are to be applied where the Council:

1) establishes a business relationship with a customer[2];
2) carries out an occasional transaction[3];
3) doubts the veracity or adequacy of documents, data or information previously obtained from the customer for the purposes of identification or verification.

To apply the due diligence measures, please answer as fully as possible the questions below.

1.	Can the Council identify this customer?	
2.	How has the identity of this customer been established? [attach documents, data or information establishing identity]	
3.	Are these documents, data or information from an independent and reliable source?	
4.	Can the Council verify the identity of the customer?	

[2] **"business relationship"** means a business, professional or commercial relationship which the Council expects, at the time the contact is established, to have an element of duration.

[3] **"occasional transaction"** means a transaction, carried out other than as part of a business relationship, amounting to 15,000 Euro or more, whether a single operation or several operations which appear to be linked. [Sterling equivalent at date of final document]

	[Through the documents referred to in Questions 2 and 3]	
5.	Is there a beneficial owner involved with the customer who is a different person or entity to the customer identified above?	
6.	What is the identity of the beneficial owner?	
7.	Can the Council verify the identity of the beneficial owner?	
8.	Does the Council doubt the veracity or adequacy of documents, data or information obtained for the purposes of identification or verification?	
9.	When were the documents, data or information obtained for the purposes of identification or verification of this customer last up-dated?	
10.	When will the documents, data or information obtained for the purposes of identification or verification of this customer next be up-dated?	
11.	What is the ownership and control structure of the beneficial owner?	
12.	Does the Council wish to establish a business relationship with this customer?	**If "No", go straight to Section C.**
13.	What is the purpose and intended nature of the business relationship?	

SECTION C: OUTCOME OF DUE DILIGENCE MEASURES	
Is the Council unable to answer any of the above questions because the customer has been unable or unwilling to provide information? If so, please give full details.	**If the answer is "Yes", the Council must not establish a business relationship or carry out an occasional transaction with this customer; it must not carry out any transaction with or for the customer through a bank account; it must terminate any business relationship with the customer AND the suspicion must be reported immediately to the MLRO.**
NOTE This pro-forma must be kept for 5 years from the end of the business relationship or occasional transaction with this customer.	