Craven District Council
Anti-Money Laundering Policy

Approved: Audit and Governance Committee 23 January 2018

1 INTRODUCTION

1.1 Money Laundering is the process by which criminally obtained money or other criminal property is exchanged for “clean” money or other assets with no obvious links to their criminal origins. The term is used for a number of offences involving the integration of “dirty” money (the proceeds of crime) into the mainstream economy. With the aim being to legitimise the possession of such monies through circulation and effectively leading to “clean” funds in exchange.

1.2 Historically, legislation seeking to prevent the laundering of the proceeds of criminal activity was aimed at professionals in the financial and investment sector, however it was subsequently recognised that those involved in criminal conduct could use a much wider range of business activities to ‘clean’ their proceeds of crime.

1.3 The Money Laundering, Terrorist Financing and Transfer of Funds (information on the Payer) Regulations 2017 (MLR 2017), which transposed the Fourth EU Money Laundering Directive into UK Law, commenced on 26 June 2017. These obligations impact on certain areas of local authority business and, as under the previous regulations 2007, require local authorities to maintain internal procedures to prevent the use of their services for money laundering. A key difference of the 2017 Regulations is to require relevant persons to adopt a more risk based approach towards anti-money laundering, particularly in the conduct of 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 the MLR 2017.

1.4 Craven District Council is committed to establishing and maintaining effective arrangements to prevent and detect attempts to launder money using Council services.

2 SCOPE OF THE POLICY

2.1 This policy applies to all officers (including agency staff) and elected members of the Council and aims to help 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. Within this policy the term employees refers to all employees and Member refers to all elected members.

2.2 Failure by an employee to comply with the procedures set out in this policy may lead to disciplinary action being taken against them. Any disciplinary action will be dealt with in accordance with the Council’s Disciplinary Policy and Procedures.

2.3 Managers and senior staff must ensure that all employees are aware of this policy. Not all staff will need a detailed knowledge covered by the legislation. However, some staff will require additional guidance to raise their awareness of the possibility of money laundering.

3 AIMS OF THE POLICY

3.1 The policy outlines the Council's arrangements:

- To nominate a Money Laundering Reporting Officer (MLRO);
- To make arrangements to receive and manage concerns of staff about money laundering and their suspicion of it, to make internal inquiries and to make reports where necessary, to the National Crime Agency NCA);
- To make those staff most likely to be exposed to or suspicious of money laundering situations aware of the requirements and obligations placed on the organisation, and on them as individuals, by the Proceeds of Crime Act, the Terrorism Act and the Money Laundering Regulations;
- To give targeted training to those considered to be most likely to encounter money laundering;
- To establish internal procedures to help forestall and prevent money laundering.

4 WHAT IS MONEY LAUNDERING?

4.1 Under the legislation there are two main types of offence which may be committed:

- Money laundering offences.
- Failure to report money laundering offences.

4.2 Money laundering activity includes:

- Acquiring, using or possessing criminal property,
- Handling the proceeds of crimes such as theft, fraud and tax evasion,
- Being knowingly involved in any way with criminal or terrorist property,
- Entering into arrangements to facilitate laundering criminal or terrorist property,
- Investing the proceeds of crime in other financial products,
- Concealing, disguising, converting, transferring criminal property or removing it from the UK,
- Transferring criminal property.

5 THE MONEY LAUNDERING REPORTING OFFICER (MLRO)

5.1 Where it is suspected that money laundering activity is taking/has taken place, an employee or Member becomes concerned that their involvement in a matter may amount to a prohibited act under the legislation, this must be disclosed as soon as practicable to the MLRO in line with procedures. The disclosure should be within "hours" of the information coming to the employee's or Member's attention, not weeks or months later.

5.2 The officer nominated to receive disclosures about suspected money laundering activity within the Council is the Chief Finance Officer. Contact details are:

Chief Finance Officer
Craven District Council
1 Belle Vue Square
Broughton Road

Skipton
BD23 1FJ
Telephone: 01757 706418
E-mail: NChick@cravendc.gov.uk

5.3 In the absence of the MLRO, or in instances where it is suspected that the MLRO themselves are involved in suspicious transactions, concerns should be raised with the Solicitor to the Council and Monitoring Officer.

6 LEGISLATION

6.1 The main UK legislation covering anti-money laundering terrorist financing is:

- Proceeds of Crime Act 2002
- Terrorism Act 2000
- Anti-Terrorism Crime and Security Act 2001
- Money Laundering Regulations 2007
- Money Laundering (Amendment) Regulations 2012
- Money Laundering (Amendment) Regulations 2015
- The Money Laundering, Terrorist Financing and Transfer of Funds (information on the Payer) Regulations 2017 (MLR 2017)

7 OBLIGATIONS ON THE COUNCIL AND INDIVIDUALS

7.1 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.

7.2 The Regulations apply to “relevant persons” acting in the course of business carried on by them in the UK. 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. However, the safest way to ensure compliance with the law is to apply it to all areas of work undertaken by the Council, therefore all employees are required to comply with the Council’s Anti Money Laundering Policy in terms of reporting concerns regarding money laundering.

7.3 Money Laundering regulations apply to cash transactions in excess of €15,000. But it is reasonable to be suspicious of any unexpected “cash” transactions over £1,000.

7.4 The Money Laundering Regulations 2017 require those organisations in the regulated sector and conducting relevant business to:

- Put in place checks, controls and procedures in order to anticipate and prevent money laundering or terrorist financing. Further information on establishing internal checks and controls can be found in section 7.6 below.

- Train staff in those procedures and in the law relating to money laundering and terrorist financing. The purpose of this policy is to promote general awareness. Specific training for those employees more likely to come across money laundering will be provided if needed.
- Appoint a nominated officer or money laundering reporting officer to receive and consider internal disclosures and to make suspicious activity reports to the National Crime Agency (NCA). Further information on the role of the nominated officers can be found in Section 5 and identifying suspicious activity at section 10 below.
- Put in place procedures to identify customers and verify the customer's identity before entering into a business relationship or transaction and to obtain information on the purpose or nature of the business relationship. These procedures are known in the regulations as "Customer Due Diligence" and also require the Council to conduct ongoing monitoring of the business relationship as appropriate. The regulations specify circumstances in which the Council is not required to undertake customer due diligence measures or must undertake enhanced measures. Further information about how and when to apply customer due diligence measures can be found in Section 7.
- Keep records obtained in establishing customers' identity and of business relationships for five years. Further information on record keeping can be found in section 8.

7.5 It is a requirement of the MLR 2017 that appropriate systems of internal control are in place to prevent activities relating to money laundering and terrorist financing. There must be management controls in place to identify the possibility that criminals may be attempting to launder money or fund terrorism, so as to enable appropriate action to prevent or report it to be taken. Management needs to consider both customer and geographical risk factors in deciding whether simplified 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. For an up to date list of such jurisdictions an officer should seek advice from the MLRO. The list of areas is currently: Afghanistan, Bosnia and Herzegovina, Guyana, Iraq, Lao, PDR, Syria, Uganda, Vanuatu, Yemen, Iran and the Democratic People's Republic of Korea.

7.6 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. 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 Council's 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 organisation.

8 CUSTOMER DUE DILIGENCE

8.1 The Council will put in place procedures to identify customers before entering into a business relationship (see below) or transaction a copy of the due diligence form is provided at Appendix B. The procedures will require the Council to:

- Identify customers and verify their identity on the basis of documents from a reliable and approved source.
- Identify where applicable the beneficial owner (see below) and take adequate measures on a risk sensitive basis to verify their identity.
- Obtain information on the purpose and intended nature of the business relationship.
- Conduct ongoing monitoring of the business relationship to ensure transactions are consistent with knowledge of the customer risk profile.
- Maintain records of all checks for 5 years.

8.2 The regulations define a business relationship as “a business, professional or commercial relationship between a relevant person and a customer, which is expected by the relevant person at the time when the contact is established to have an element of duration”.

8.3 “Beneficial owners” are the individuals who ultimately own or control the customer or on whose behalf a transaction or activity is being conducted.

8.4 If satisfactory evidence of a customer’s identity at the outset cannot be obtained, then the business relationship and or transaction can NOT proceed any further.

8.5 In certain circumstances, the Council is not required to apply any customer due diligence. The Council will not have to verify the identity of customers or seek additional information about the nature or purpose of business relationships where:

- The customer is a public authority in the UK.
- The customer is a credit or financial institution that is subject to regulations.
- The customer is a listed company subject to disclosure provisions.
- The customer is a European Community institution.

8.6 The Council is required to undertake additional or enhanced customer due diligence measures on a risk sensitive basis. This includes where:

- The customer has not been physically present for identification.
- The customer is a politically exposed person or an immediate family member or close associate of a politically exposed person (a “politically exposed person” is an individual who has, or has had in the previous year, a high political profile, or holds, or has held in the previous year, public office overseas).
- In situations which by their nature can present a higher risk of money laundering or terrorist financing.

9 PENALTIES FOR FAILURE TO COMPLY

9.1 Failing to comply with the regulations could lead to a prosecution which could result in unlimited fines and/or a prison sentence of up to two years.

9.2 Failing to comply with the regulations could also result in civil financial penalties (a different sanction leading to prosecution leading to a fine).

10 REPORTING AND RECORD KEEPING

Reporting a Concern to the MLRO

10.1 Employees or Members who know or suspect that they may have encountered criminal activity and that they are at risk of contravening the money laundering legislation, should contact the MLRO to advise her of their concerns.

10.2 The disclosure should be at the earliest opportunity of the information coming to your attention, not weeks or months later.

10.3 A flow chart illustrating the procedure for reporting money laundering is at Appendix C. More information about making a report to the MLRO is detailed at Appendix D, with a Money Laundering Disclosure Form attached.

Reporting to the National Crime Agency

10.4 The initial discussion / disclosure will be noted by the MLRO, and she will promptly evaluate this and determine whether it is appropriate to report it to the National Crime Agency (NCA).

10.5 If a report is made then the relevant NCA forms must be completed by the MLRO. Up to date 'Suspicious Activity Report' forms can be downloaded from the NCA website at: http://www/nationalcrimeagency.gov.uk/

10.6 In the event that a report is not submitted online, a form can be downloaded from the following website: http://www.nationalcrimeagency.gov.uk/publications/36-ukfiu-appendix-2-disclosure-report-detail/file

10.7 If no report is made, the reason must be recorded by the MLRO.

10.8 All disclosure reports referred to the MLRO and reports made to the NCA must be retained by the MLRO in a confidential file for a minimum of 5 years. The Money Laundering Disclosure Form at Appendix D should be used to facilitate the recording of any action taken.

10.9 The MLRO or deputy will commit 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 NCA.

Record Keeping

10.10 Each service unit of the Council conducting relevant business must maintain records of:

- Client identification evidence obtained; and
- Details of all relevant business transactions carried out for clients.
- For at least five years. This is so that they may be used as evidence in any subsequent investigation by the authorities into money laundering and also demonstrates the Council's compliance with the regulations.

10.11 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, for example distinguishing the client and the relevant transaction and recording in what for the funds were received or paid. In practice the service units of the Council will be routinely making records of work carried out for clients in the course of normal business and these should suffice in this regard.

10.12 The MLRO will keep a record of all referrals received and any action taken to ensure an audit trail is maintained.

11 RISK REGISTER

11.1 Regulation 18 of the MLR 2017 requires a written risk assessment to identify and assess the risk of money laundering and terrorist financing that the Council faces.

11.2 Whilst all employees must be aware of the existence of the Anti-Money Laundering Policy, Procedures and Reporting arrangements, it is possible to identify those areas of the Council most at risk to potential involvement in money laundering.

11.3 In order to identify the "at risk" areas the MLRO will maintain a Money Laundering Risk Register. Under MLR 2017 risk mitigation policies must be in writing and be proportionate to the risks identified. The steps followed to establish the risk register were to:

- Identify the money laundering and terrorist financing risks that were relevant to the Council.
- Assess the risks presented by particular customers, products and services, delivery channels and geographical area.
- Design and implement controls to manage and mitigate the assessed risks.

11.4 In carrying out the risk assessment information on money laundering and terrorist financing risks made available by the Law Society and/or SRA, and risk factors relating to:

- customers
- the countries or geographic areas where the Council operates
- products and services

- transactions and
- delivery channels

11.5 Risks will be reviewed continuously as part of the annual review of the Council Risk Register.

12 TRAINING AND PUBLICITY

12.1 The Council will take appropriate measures to ensure that all employees are made aware of the law relating to money laundering. Targeted training will be arranged at appropriate intervals for key Officers most likely to be affected by the legislation, Finance, Legal and Local Taxation.

12.2 Appropriate training will also be made available to Members.

12.3 It is the duty of Officers and Members to report all suspicious transactions whether they have received their training or not.

13 POLICY REVIEW

13.1 The policy will be kept under review at appropriate intervals in line with the Council's Whistleblowing Policy and Anti-Fraud and Corruption Policy and any changes to legislation.

14 CONCLUSIONS

14.1 The Money Laundering legislation is complex. Given a local authority's legal position with regard to legislative requirements this policy has been written as a safeguard and to enable the Council to meet its legal obligations. The policy represents an appropriate response to the level of risk the Council faces of money laundering offences.

ACTIVITIES WHICH COULD BE INDICATIVE OF MONEY LAUNDERING

1. The payment of a substantial sum in cash or by debit card (over £10,000).

2. A secretive customer: e.g. refuses to provide requested information without a reasonable explanation.

3. Concerns about the honesty, integrity, identity or location of a client.

4. Illogical third party transactions: unnecessary routing or receipt of funds from third parties or through third party accounts.

5. Involvement of an unconnected third party without a logical reason or explanation.

6. Substantial overpayments by a client, at least €15,000. NB a payment for less than this may still be money laundering & should be reported, however, it may be a fraud using a stolen card rather than money laundering.

7. Large unsolicited payments in advance or deposits, which may ultimately need to be returned. NB This may be a fraud using a stolen card rather than money laundering.

8. Absence of an obvious source of legitimate funds.

9. Movement of funds overseas, particularly to a higher risk country or tax haven.

10. Where, without reasonable explanation the size, nature and frequency of transactions or instructions (or size, location or type of client) is out of line with normal expectations.

11. A transaction without obvious legitimate purpose or which appears to uneconomic, inefficient or irrational.

12. Requests for release of client account details other than in the normal course of business.

13. Companies and trusts: extensive use of corporate structures and trusts in circumstances where the client's needs are inconsistent with the use of such structures.

14. Poor business records or internal accounting controls.