LONDON BOROUGH OF ENFIELD

ANTI-MONEY LAUNDERING POLICY

MARCH 2026

Reviewed	M Cameron	February 2026
Next Review	Head of Internal Audit	January 2029

Anti-Money Laundering Policy

1 Introduction

1.1 This Policy sets out the arrangements by which Enfield Council ("the Council") will prevent, detect and report suspected money laundering and terrorist financing, and ensure compliance with relevant legislation.

1.2 The Council is committed to maintaining the highest standards of integrity and to preventing its services from being used to launder the proceeds of crime or to facilitate terrorist financing.

1.3 While public authorities are not legally obliged to apply the provisions of money laundering regulations, the Chartered Institute of Public Finance and Accountancy (CIPFA) recommends that they employ policies and procedures to deal with the growing threat of terrorist financing, money laundering and other financial crimes.

2 Legislative and Regulatory Framework

2.1 This Policy is informed by, and must be read in conjunction with, the following legislation and guidance (as amended from time to time):

- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017
- Money Laundering and Terrorist Financing (Amendment) Regulations 2019
- The Money Laundering and Terrorist Financing (Amendment) (No.2) Regulations 2022
- Proceeds of Crime Act 2002 (POCA)
- Serious Organised Crime and Police Act 2005
- Terrorism Act 2000
- Criminal Finances Act 2017
- Fraud Act 2006
- Bribery Act 2010
- Data Protection Act 2018 and UK GDPR

2.2 The legislation in this area is detailed and complex. If you require further advice, please contact the Money Laundering Reporting Officer (MLRO) **(see section 15)**.

3 Scope

3.1 This policy applies to the following individuals and groups in relation to the Council and its subsidiary companies:

- All Council employees
- Agency, and temporary staff
- Members
- Contractors and consultants

3.2 For the purposes of this Policy, any reference to “staff” includes all of the above.

3.3 Failure to comply with this Policy may result in:

- Disciplinary action (for employees and Members)
- Termination of contracts (for agency and temporary workers and contractors)
- Referral to external enforcement bodies where appropriate.

4 What is Money Laundering?

4.1 Money laundering refers to activities intended to conceal or disguise the proceeds of crime so that they appear to have originated from legitimate sources. This commonly involves placing illegally obtained funds or assets into an organisation’s systems or transactions to give them the appearance of lawful origin.

Three elements constitute money laundering:

- **Concealing, disguising, converting, transferring or removing criminal property** (s.327 POCA)
- **Entering into or becoming concerned in arrangements** which you know or suspect facilitate the acquisition, retention, use or control of criminal property (s.328 POCA)
- **Acquiring, using or possessing criminal property** (s.329 POCA).

These offences are not committed where the individual did not know or suspect that they were dealing with the proceeds of crime.

It is also a criminal offence to:

- **Fail to disclose** knowledge or suspicion of money laundering where you acquired such knowledge or suspicion in the course of your work (s.330 POCA)
- **“Tip off”** a person that a disclosure has been made (s.333A POCA)
- **Prejudice** an investigation (s.342 POCA).

These offences are not committed if a report of the suspicious activity is made promptly to the MLRO.

5 Policy Statement

5.1 Our policy is to take all reasonable steps to:

- **Prevent**, wherever possible, the Council, its staff, Members, contractors and subsidiary companies from being exposed to money laundering

- **Identify** areas where there is a potential risk of money laundering occurring
- Ensure **compliance** with legal and regulatory requirements, particularly in relation to the reporting of actual or suspected cases.

5.2 To achieve this, the Council will:

- Make this policy available to staff
- Provide fraud awareness training on the Council's e learning platform, supplemented by face-to-face training where required
- Undertake risk-based, targeted internal audit work to provide assurance on compliance
- Ensure the Money Laundering Reporting Officer is supported by a nominated deputy, to ensure money laundering suspicions are reported in line with legal and regulatory requirements
- Provide updates and assurance to senior management and Members, via Assurance Board and Audit Committee on the Council's compliance with and implementation of the Money Laundering Regulations.

6 Governance and Key Roles

6.1 Money Laundering Reporting Officer (MLRO) and Compliance Officer

The Council's MLRO is the Head of Internal Audit, Marion Cameron who is responsible for:

- Receiving and assessing internal disclosures of suspected money laundering
- Making Suspicious Activity Reports (SARs) to the National Crime Agency where appropriate
- Liaising with law enforcement and regulatory bodies
- Maintaining appropriate records
- Providing advice and guidance to staff.

6.2 Deputy Money Laundering Reporting Officer (MLRO)

In the absence of the MLRO, the Council's Counter Fraud Manager is authorised to deputise.

6.3 Compliance Officer

Overall responsibility for compliance with this Policy rests with the Council's Section 151 Officer / Chief Finance Officer, supported by Internal Audit and Counter Fraud. For the purposes of the Policy, the Section 151 Officer/Chief Finance Officer is the Compliance Officer.

The Compliance Officer has oversight of activities falling within the scope of the Money Laundering Regulations and is specifically responsible for ensuring that appropriate due diligence arrangements are in place within services exposed to the risk of money laundering.

Refer to **Section 15** for contact details.

7 Customer Due Diligence (CDD)

7.1 Customer Due Diligence is necessary to check the identity of the customer or client where the Council or its subsidiary companies:

- Establish a business relationship with a customer (or another party in a property sale)
- Suspect money laundering or terrorist financing
- Have doubts about a customer's identification information
- Need to verify existing customers — for example, if their circumstances change
- Carry out an 'occasional transaction' worth €15,000 (approx. £13k) or more.

7.2 In such circumstances CDD must be followed before any business is undertaken for that client. Verification may be carried out during the establishment of the business relationship where it is necessary not to interrupt the normal conduct of business and there is little risk of money laundering/terrorist financing occurring, provided that the verification is completed as soon as practicable after contact is first established.

7.3 Customer due diligence means taking steps to identify your customers and checking they are who they say they are. In practice this means obtaining a customer's:

- Name
- Photograph on an official document which confirms their identity
- Residential address or date of birth.

The best way to do this is to ask for:

- A government issued document like a passport
- Utility bills
- Bank statements
- Other official documents.

Other sources of customer information include the electoral register and information held by credit reference agencies such as Experian and Equifax.

You also need to identify the 'beneficial owner' in certain situations. This may be because someone else is acting on behalf of another person in a particular transaction, or it may be because you need to establish the ownership structure of a company, partnership or trust.

The beneficial owner is usually 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.

If you have doubts about a customer's identity, you must stop dealing with them until you're sure.

7.4 Enhanced Due Diligence

In some situations you must carry out 'enhanced due diligence'. These situations are:

- When the customer is not physically present when you carry out identification checks;
- When you enter into a business relationship 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 — find the list of high risk third countries on the EU's website;
- Any other situation where there's a higher risk of money laundering.

7.5 The Compliance Officer is responsible for ensuring appropriate due diligence arrangements are in place within services exposed to money laundering risk

8 Staff Responsibilities

8.1 All staff **must**:

- Be vigilant to the risk of money laundering
- Familiarise themselves with this policy
- Complete mandatory training where required
- Report suspicions promptly.

8.2 Staff **must not**:

- Investigate suspicions themselves
- Delay reporting
- Discuss concerns with the individual(s) involved, even where consent to proceed with the transaction has been given, as this may constitute 'tipping off'.

Failure to act appropriately may expose both the individual and the Council to criminal liability.

9 Reporting Suspicions (Internal Disclosure Procedure)

9.1 Where a member of staff knows or suspects, or has reasonable grounds to know or suspect, that money laundering or terrorist financing is taking place or has taken place, or becomes concerned that their involvement in a matter may constitute a prohibited activity under the legislation, they must report this as soon as practicable to the MLRO or Deputy MLRO.

9.2 Disclosures must be made using the Council's Disclosure Reporting form to the Money Laundering Reporting Officer, available on the Counter Fraud intranet page here. You must include:

- Full details of the concern
- Relevant transactions, amounts and dates
- Any supporting documentation.

9.3 Once a disclosure has been made:

- You must take no further action (including further enquiries) without MLRO direction
- The transaction must not proceed unless authorised.

9.4 Upon receipt of a disclosure report, the MLRO will advise you of the timescale for providing a response to you. Usually this will be within 10 working days.

10 Suspicious Activity Reports (SARs)

10.1 The MLRO will assess all disclosures and determine whether a SAR must be submitted to the National Crime Agency (NCA).

10.2 Where consent is required from the NCA to proceed with a transaction, the **transaction must not proceed until consent is received** or deemed consent applies following the expiry of the relevant statutory time limits without objection from the NCA.

10.3 The existence of a SAR must remain confidential at all times.

11 Record Keeping

11.1 Records relating to:

- CDD
- Business transactions
- Internal disclosures
- SAR decisions

must be retained for **at least six years**, in line with legislative requirements.

11.2 Records must be stored securely and in accordance with data protection legislation.

12 Training and Awareness

12.1 The Council will ensure that:

- Appropriate AML training is provided to relevant staff
- Training is proportionate to role and risk
- Refresher training is provided periodically.

13 Monitoring and Review

13.1 Compliance with this Policy will be monitored through:

- Internal Audit activity
- Counter Fraud investigations
- Management assurance.

13.2 This Policy will be reviewed at least **every three years**, or sooner if required due to legislative or organisational change.

14 Related Policies

- Counter Fraud and Corruption Policy
- Whistleblowing Policy
- Anti-Bribery & Corruption Policy
- Employee and Members Codes of Conduct
- Financial Regulations.

15 Contact Details

15.1 If you have concerns or require further advice, you should contact:

Duty	Position	Name	Email	Phone
MLRO	Head of Internal Audit	Marion Cameron	Marion.Cameron@enfield.gov.uk	020 8132 1065
Compliance Officer	Chief Finance Officer	Olga Bennet	Olga.Bennet@enfield.gov.uk	020 4522 9995