[COMPANY NAME]

Anti-Money Laundering & Counter-Terrorist Financing Policy

CONFIDENTIAL

Policy Version: 1.0
Effective Date: 18 February 2026
Next Review Date: [Date]
Policy Owner: Money Laundering Reporting Officer (MLRO)
Classification: Confidential

Table of Contents

1. Introduction and Purpose

This Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) Policy sets out the framework, principles, and procedures adopted by [Company Name] (hereinafter referred to as "the Company") to prevent the use of its products and services for money laundering, terrorist financing, proliferation financing, and other forms of financial crime.

The policy is designed to ensure compliance with all applicable laws, regulations, and industry standards, and to protect the Company, its employees, customers, and stakeholders from the risks associated with financial crime.

1.1 Scope

This policy applies to all directors, officers, employees (permanent and temporary), contractors, agents, and third parties acting on behalf of the Company across all business units, subsidiaries, and jurisdictions in which the Company operates.

1.2 Policy Objectives

- Establish a robust framework for identifying, assessing, and managing money laundering and terrorist financing risks
- Ensure compliance with applicable legislation, regulations, and supervisory guidance
- Define clear roles, responsibilities, and reporting lines for AML/CTF governance
- Set out customer due diligence (CDD) and enhanced due diligence (EDD) requirements
- Establish procedures for monitoring, detecting, and reporting suspicious activity
- Provide a framework for sanctions screening and compliance
- Ensure adequate staff training and awareness programmes are in place
- Maintain comprehensive record-keeping in accordance with legal requirements

2. Legal and Regulatory Framework

The Company is committed to compliance with all applicable AML/CTF legislation and regulatory requirements. The following is a non-exhaustive list of the principal legislation, regulations, and guidance that inform this policy:

2.1 Primary Legislation

- Proceeds of Crime Act 2002 (POCA) — principal UK legislation creating money laundering offences and establishing the suspicious activity reporting regime
- Terrorism Act 2000 — offences relating to terrorist financing, including fundraising, use and possession, and funding arrangements
- Sanctions and Anti-Money Laundering Act 2018 (SAMLA) — framework for UK autonomous sanctions regimes
- Anti-terrorism, Crime and Security Act 2001 — provisions on freezing orders and disclosure of information

2.2 Regulations and Statutory Instruments

- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs) as amended
- The Sanctions and Anti-Money Laundering Act 2018 (Implementation of Sanctions) Regulations

2.3 Regulatory Guidance

- Joint Money Laundering Steering Group (JMLSG) Guidance for the UK Financial Sector
- Financial Conduct Authority (FCA) Financial Crime Guide and Handbook provisions
- HM Treasury National Risk Assessment of Money Laundering and Terrorist Financing
- Financial Action Task Force (FATF) Recommendations and Guidance Papers
- Relevant European Banking Authority (EBA) Guidelines where applicable

Note: Where the Company operates in jurisdictions outside the United Kingdom, it shall also comply with local AML/CTF legislation, regulations, and supervisory guidance. In the event of conflict between UK and local requirements, the higher standard shall prevail unless doing so would contravene local law.

3. Governance and Responsibilities

3.1 Board of Directors

The Board has ultimate responsibility for the Company's AML/CTF framework. The Board shall ensure that adequate resources, systems, and controls are in place to manage money laundering and terrorist financing risks effectively. The Board shall approve this policy and receive regular reports on AML/CTF matters, including the findings of the annual compliance review.

3.2 Money Laundering Reporting Officer (MLRO)

The Company shall appoint a Money Laundering Reporting Officer (MLRO) at a sufficiently senior level, with appropriate authority, independence, and resources to discharge their duties effectively. The MLRO is responsible for:

- Receiving, evaluating, and where appropriate filing Suspicious Activity Reports (SARs) with the National Crime Agency (NCA)
- Acting as the primary point of contact with relevant regulatory and law enforcement bodies
- Overseeing the implementation and effectiveness of the AML/CTF framework
- Producing and presenting the annual MLRO report to the Board
- Ensuring that the business-wide risk assessment is kept current
- Advising senior management on emerging money laundering and terrorist financing risks

3.3 Deputy MLRO

A Deputy MLRO shall be appointed to discharge the duties of the MLRO in their absence. The Deputy MLRO shall have the same access to information, systems, and resources as the MLRO.

3.4 Senior Management

Senior management is responsible for ensuring that AML/CTF policies and procedures are embedded within their respective business areas, that adequate resources are allocated, and that staff are appropriately trained and aware of their obligations.

3.5 All Staff

Every employee has a personal legal obligation to report knowledge or suspicion of money laundering or terrorist financing. Failure to report may constitute a criminal offence under POCA or the Terrorism Act 2000. All staff must complete mandatory AML/CTF training and cooperate with compliance enquiries.

4. Risk Assessment

4.1 Business-Wide Risk Assessment

The Company shall conduct and maintain a comprehensive business-wide risk assessment (BWRA) that identifies and assesses the money laundering and terrorist financing risks to which the Company is exposed. The BWRA shall consider risks arising from customers, products and services, delivery channels, geographic locations, and the nature and complexity of transactions.

The BWRA shall be reviewed and updated at least annually, or more frequently where there are material changes to the business, its customer base, product offerings, or the external risk environment.

4.2 Customer Risk Assessment

Each customer relationship shall be assigned a risk rating based on a documented methodology. Risk ratings shall be reviewed periodically and updated as necessary in response to changes in the customer's profile, behaviour, or transaction patterns.

Risk Level	Customer Type	EDD Required	Review Frequency
High	PEPs, high-risk jurisdictions, complex structures	Yes - enhanced due diligence	Every 6 months
Medium	Non-resident customers, higher value transactions	Case-by-case basis	Annually
Low	Domestic individuals, established businesses	No - standard CDD sufficient	Every 3 years

4.3 Risk Factors

The following non-exhaustive risk factors shall be considered when assessing customer and transaction risk:

4.3.1 Higher-Risk Indicators

- Customers who are, or are associated with, Politically Exposed Persons (PEPs)
- Customers established or operating in high-risk jurisdictions identified by FATF, the EU, or HM Treasury
- Complex or opaque ownership structures, including nominee arrangements and bearer shares
- Transactions that are unusually large, complex, or have no apparent lawful economic purpose
- Cash-intensive businesses or sectors identified as higher risk in the National Risk Assessment
- Customers requesting unusual levels of secrecy or reluctant to provide identification information
- Correspondent banking relationships involving high-risk jurisdictions

4.3.2 Lower-Risk Indicators

- Domestic customers with established identities and transparent ownership
- Publicly listed companies subject to regulatory disclosure requirements
- Government bodies and public sector entities from low-risk jurisdictions
- Regulated financial institutions from equivalent jurisdictions

5. Customer Due Diligence (CDD)

5.1 General Principles

The Company shall not establish a business relationship or carry out an occasional transaction unless satisfactory CDD measures have been applied. Where CDD cannot be completed to a satisfactory standard, the business relationship shall not proceed, and consideration shall be given to whether a SAR should be filed.

5.2 Standard CDD Requirements

Standard CDD shall be applied to all customers and shall include the following:

- Identification: Obtaining and recording the customer's full legal name, date of birth (for individuals), registered address, and other identifying information as appropriate
- Verification: Verifying the customer's identity using reliable and independent sources, documents, or electronic verification services
- Beneficial Ownership: Identifying any beneficial owners holding 25% or more of shares, voting rights, or ownership interest, and verifying their identity
- Purpose and Nature: Understanding the purpose and intended nature of the business relationship
- Source of Funds: Establishing the source of funds and, where appropriate, the source of wealth
- Ongoing Monitoring: Conducting ongoing monitoring of the business relationship to ensure that transactions are consistent with the customer's known profile

5.3 Enhanced Due Diligence (EDD)

EDD measures shall be applied in all cases where the risk of money laundering or terrorist financing is assessed as higher than standard, including but not limited to the following situations:

- The customer is a PEP, a family member of a PEP, or a known close associate of a PEP
- The customer is established or operates in a high-risk third country identified by FATF or HM Treasury
- The transaction or business relationship is unusually complex or has no apparent economic or lawful purpose
- There are grounds for suspicion of money laundering or terrorist financing, irrespective of transaction value

EDD measures may include, but are not limited to: obtaining additional identification information, conducting enhanced background checks, establishing the source of wealth, obtaining senior management approval for the business relationship, and increasing the frequency and intensity of ongoing monitoring.

5.4 Simplified Due Diligence (SDD)

Where a customer presents a demonstrably lower risk of money laundering or terrorist financing, the Company may apply SDD measures, provided that this is permitted by the applicable risk assessment and regulatory framework. SDD does not exempt the Company from monitoring the business relationship for unusual or suspicious activity.

5.5 Reliance on Third Parties

The Company may rely on CDD measures carried out by eligible third parties in accordance with Regulation 39 of the MLRs. However, ultimate responsibility for CDD compliance remains with the Company. Formal agreements shall be in place with any third party upon which reliance is placed, and the Company shall satisfy itself that the third party applies CDD measures and retains records equivalent to those required under the MLRs.

6. Ongoing Monitoring and Transaction Surveillance

6.1 Ongoing Monitoring

The Company shall apply ongoing monitoring to all business relationships, commensurate with the assessed level of risk. Ongoing monitoring includes scrutiny of transactions to ensure they are consistent with the Company's knowledge of the customer, their business and risk profile, and where necessary, the source of funds.

6.2 Transaction Monitoring

The Company shall implement systems and controls — whether automated, manual, or a combination of both — to detect transactions that are unusual, complex, large, or otherwise inconsistent with the expected pattern of activity. The transaction monitoring framework shall be calibrated to the Company's risk appetite and reviewed periodically.

6.3 Triggers for Review

The following events shall trigger a review of the customer's risk rating and CDD information:

- A significant or unexpected change in the customer's transaction pattern or volume
- Adverse media or intelligence reports concerning the customer
- Changes to the customer's ownership structure, senior management, or nature of business
- A request from law enforcement, a regulator, or the NCA
- Changes in the risk profile of the customer's jurisdiction of incorporation or operation
- The customer's CDD information reaching its scheduled review date

7. Suspicious Activity Reporting

7.1 Obligation to Report

Under POCA and the Terrorism Act 2000, it is a criminal offence to fail to report knowledge or suspicion of money laundering or terrorist financing where such knowledge or suspicion arises in the course of business. All employees must report any such knowledge, suspicion, or reasonable grounds for suspicion to the MLRO without delay.

7.2 Internal Reporting Procedure

The internal reporting process follows a structured escalation path to ensure timely and appropriate assessment of suspicious activity:

Step	Action	Responsible Party	Timeframe
1. Detection	Identify suspicious activity	All staff	Immediately
2. Internal Report	Submit internal SAR to MLRO	Reporting employee	Same business day
3. Assessment	MLRO evaluates report and supporting evidence	MLRO / Deputy MLRO	Within 3 business days
4. Filing	Submit SAR to relevant FIU / NCA	MLRO	As soon as practicable

5. Record	Document decision and retain records	MLRO	Ongoing

7.3 Consent Regime

Where the Company is required to obtain appropriate consent from the NCA before proceeding with a transaction (a “defence against money laundering”), the MLRO shall submit a Defence Against Money Laundering (DAML) request and await consent before authorising the transaction to proceed. Staff must not proceed with a transaction where consent has been requested but not yet granted, unless the relevant statutory notice period has expired.

7.4 Tipping Off

It is a criminal offence under section 333A of POCA to disclose to any person that a SAR has been made, or that a money laundering investigation is being, or may be, carried out, where such disclosure is likely to prejudice the investigation. All employees must exercise extreme caution in their communications with customers and third parties in such circumstances. Any doubt regarding tipping off obligations should be referred to the MLRO immediately.

8. Sanctions Compliance

8.1 Overview

The Company is committed to complying with all applicable sanctions regimes, including those imposed by the United Kingdom (through OFSI), the European Union, the United Nations, and the United States (OFAC) where applicable. Non-compliance with sanctions is a strict liability criminal offence.

8.2 Screening

The Company shall screen all customers, beneficial owners, and connected parties against relevant sanctions lists at the point of onboarding and on an ongoing basis. The screening process shall also be triggered by updates to sanctions lists and by material changes to customer information.

8.3 Sanctions Matches

Where a potential sanctions match is identified, the transaction shall be immediately frozen and escalated to the MLRO and Compliance team. No funds shall be released, and no services shall be provided, until the match has been resolved. Confirmed matches shall be reported to the Office of Financial Sanctions Implementation (OFSI) without delay.

9. Record Keeping

9.1 Retention Requirements

The Company shall retain all CDD records, transaction records, and supporting documentation for a minimum period of five years from the date the business relationship ends or the date of the occasional transaction, in accordance with Regulation 40 of the MLRs. Records relating to SARs and internal investigations shall be retained for a minimum of five years from the date of the report.

9.2 Record Format and Accessibility

Records shall be maintained in a manner that allows them to be made available promptly to law enforcement, the NCA, or the relevant supervisory authority upon request. Records may be held in electronic or physical form, provided they are accurate, complete, and retrievable in a timely manner.

10. Training and Awareness

10.1 Training Programme

The Company shall maintain a comprehensive AML/CTF training programme to ensure that all staff are aware of their legal obligations and the Company's policies and procedures. Training shall be tailored to the roles and responsibilities of individual staff members.

Audience	Training Type	Frequency	Delivery Method
All new employees	AML/CTF induction	Within 30 days of joining	E-learning + in-person
Front-line staff	CDD and transaction monitoring	Annually	Workshop / e-learning
Senior management	Governance, risk appetite, regulatory updates	Annually	Briefing / seminar
MLRO / Compliance	Advanced AML, sanctions, typologies	Ongoing / quarterly	External courses / CPD

10.2 Training Records

Records of all training completed, including content, date, duration, attendees, and assessment results, shall be maintained and made available for regulatory review upon request.

11. Policy Review and Updates

This policy shall be reviewed at least annually by the MLRO and approved by the Board. Reviews may be triggered more frequently by material changes in legislation, regulation, supervisory guidance, the Company's business activities, or the external risk environment.

All amendments to this policy shall be recorded in the version control table and communicated to relevant staff in a timely manner.

12. Whistleblowing and Non-Retaliation

The Company encourages all employees to report concerns regarding potential money laundering, terrorist financing, or breaches of this policy without fear of retaliation. The Company's whistleblowing policy provides protections for individuals who make disclosures in good faith. Reports may be made to the MLRO, the Compliance team, or through the Company's confidential whistleblowing channel.

13. Enforcement and Disciplinary Action

Breaches of this policy may result in disciplinary action, up to and including dismissal, and may also give rise to criminal liability. The Company reserves the right to report breaches to the relevant regulatory or law enforcement authorities.

14. Document Control

Version	Date	Author	Changes
1.0	18 February 2026	[MLRO Name]	Initial policy creation

Policy Approval

Role	Name	Signature / Date
MLRO	[Name]	
Chief Executive Officer	[Name]	
Board Chair	[Name]	