MacLaren
& PARTNERS

ANTI-MONEY LAUNDERING
POLICY and PROCEDURE MANUAL

January 2026

MACLAREN & PARTNERS is committed to the prevention of money laundering and terrorist financing in accordance with the relevant UK legislation. All employees are required to be fully familiar with, and comply with, the procedures set out in this Anti-Money Laundering (AML) Policy and Procedure Manual.

This manual incorporates the requirements of the following primary legislation:

- Proceeds of Crime Act 2002 (as amended)
- Bribery Act 2010
- Terrorism Act 2000
- Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (as amended)

FCSCOMPLIANCE
Property Division

Chapter 1 - ABOUT THE MANUAL AND THE FIRM

Purpose

The purpose of this document is to provide detailed policies and procedures to ensure that MACLAREN & PARTNERS is able to meet its legal obligation to deter, detect and disrupt money laundering or terrorist financing and to ensure compliance with the requirements of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (ML regs). This policy adheres to: The Proceeds of Crime Act 2002, The Terrorism Act 2000 and Guidance from HM Revenue & Customs (HMRC) as the supervisory authority.

How to use this Policy

All relevant employees must read and understand this Policy & Procedure Manual upon joining the Firm. This manual serves as a reference guide and should be consulted whenever AML-related queries arise. While it may not address every possible situation, it establishes the key principles and operating standards that all staff must follow. Supplementary reference guides, including government issued AML legislation, guidance, and the National Risk Assessment, are available to all staff for further understanding.

Responsibilities for maintenance and training

The Nominated Officer (NO) / Money Laundering Reporting Officer (MLRO) and/or the Senior Manager are responsible for maintaining this Policy & Procedure Manual, ensuring it remains current and compliant with legislative and regulatory requirements. All staff members share a duty to support this process by promptly notifying the NO, MLRO, or Senior Manager of any potential amendments or procedural updates that may be necessary. Furthermore, all employees receive appropriate Anti-Money Laundering (AML) training on a regular basis to ensure they remain informed of the latest legal requirements, industry best practices, and emerging risks or trends in relation to AML.

Distribution and Accessibility

A securely maintained electronic copy of this Policy & Procedure Manual is currently stored on the Firm's computer system. The Nominated Officer (NO) / Money Laundering Reporting Officer (MLRO) will ensure that the manual is readily accessible to all members of staff at all times. Whenever a revised version of the manual is issued, it will replace the previous version in full so that only the most current policies and procedures are in circulation.

Queries

All queries regarding the content of this manual should be directed to the Firm's Nominated Officer (NO) / Money Laundering Reporting Officer (MLRO). Where the NO/MLRO is unable to provide a definitive response, they will obtain guidance from the relevant regulatory authority responsible for anti-money laundering compliance, such as HMRC, the National Crime Agency, or the Firm's appointed external AML consultancy, FCS Compliance Ltd.

Updates and amendments

The Firm reviews this manual regularly, at least annually, and more frequently when required, for example, to reflect organisational changes, legislative updates, or the development or revision of international standards. Updates and amendments are prepared in conjunction with FCS Compliance Ltd and approved by the Nominated Officer (NO) / Money Laundering Reporting Officer (MLRO).

Once approved, the amendments are incorporated into our manual, and the NO/MLRO distributes the revised version to all staff via email. The accompanying communication clearly outlines the changes and amendments made, ensuring that all staff remain fully informed of updates to the Firm's policies and procedures.

In implementing these policies and procedures, the Firm takes into account the following risk categories, as identified in government guidance and the National Risk Assessment:

- Customers and counterparties
- Countries or geographic risks
- Products and services provided
- Delivery channel and transaction risks
- Staff training/systems/reporting

The Firm is committed to full compliance with all legislation designed to combat money laundering and terrorist financing. This commitment includes maintaining effective controls to

mitigate these risks and providing appropriate staff training to ensure the timely identification of potential issues in each risk area.

This Firm assesses terrorist financing risk as low, this is based on our client profile and the National Risk Assessment, but we remain committed to reporting any related suspicious activity in line with legal obligations.

Firm Description

This Firm, Maclaren & Partners LLP, trades under the name Maclaren & Partners. It was incorporated on 29 June 2010 and is registered in England and Wales under Firm number OC356056. The business operates in commercial sales and acquisitions.

Maclaren & Partners is a small-sized firm with a single office based in London. The firm operates across the UK, providing services in relation to commercial properties nationwide. The Firm's activities focus solely on commercial property sales and acquisitions for individual and corporate clients seeking business opportunities in the UK.

The Firm employs 3 staff members in total, including 01 Senior manager. The office in London provides services to clients operating in the commercial property sector, with compliance oversight managed centrally.

The NO/MLRO regularly reviews how the Firm meets its obligations, including the reporting of suspicious activity. The NO/MLRO's responsibilities include receiving and assessing internal reports and liaising with relevant external agencies.

This Firm understands that should any elements of its business processes change to the extent that it includes any additional areas of business not expressly referred to in this policy, the policies, procedures and risk assessment will be amended accordingly.

Chapter 2 – REGULATED ESTATE AGENCY BUSINESS & OUR RISK BASED APPROACH

Regulatory Registration and AML Supervision

We operate as an estate agency and /or letting agent business and are:

- Appropriately registered with HM Revenue & Customs (HMRC) for the purposes of AML supervision - Registration Number: XPML00000173586

Key AML Compliance Roles

- Money Laundering Reporting Officer (MLRO) / Nominated Officer (NO): Duncan Maclaren (partner)

Firm Risk

Proliferation and Terrorist Finance Risks

In accordance with UK Government findings, the real estate sector is generally assessed as presenting a low inherent risk of exposure to proliferation financing and terrorist financing. While we remain alert to the possibility of such activities, our primary area of exposure is recognised to be the risk of money laundering through property transactions.

Risk Level

The UK Government has assessed property as having a high risk of exposure to money laundering and deemed Estate Agency Businesses as a medium risk with a slightly increased risk since 2020. Letting agents generally are now considered to be a low risk however regulated letting agency businesses are more likely to be exposed to high risk clients. His Majesty's Treasury (HMT) has provided specific guidance which was updated in January 2024 (see Reference Guide).

Following a detailed evaluation of the risk factors relevant to the size, scale, and nature of our operations, we have determined our overall firm-wide risk level to be **Medium**.

This assessment reflects:

- The limited occurrence of suspicious behaviour or red flags identified within our business to date; and
- The comprehensive risk mitigation measures currently implemented to detect, prevent, and manage potential money laundering or terrorist financing risks.

The Firm adopts a risk-based approach in the conduct of all transactions, ensuring that its anti-money laundering procedures and Firm-Wide Risk Assessment (FWRA) are robust, proportionate, and aligned with current regulatory standards. The FWRA and associated procedures will be formally reviewed on an annual basis, and revised without delay in response to any significant changes to:

- The Firm's business operations or internal processes
- Applicable legislation or regulation, including updates to the UK National Risk Assessment
- Guidance issued by HM Treasury (HMT) or HM Revenue & Customs (HMRC)

Following each review, all relevant documents will be updated to reflect the most current requirements, ensuring the Firm's AML framework remains effective and fully compliant.

Effectiveness of AML controls and Risk Mitigation

As of 2026, the Firm's firm-wide risk profile for Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) is assessed as **medium**. This overall assessment reflects the effectiveness of the Firm's existing policies, procedures, and control measures in identifying, managing, and mitigating exposure to these risks (refer to the Risk Assessment section).

Our primary risk mitigation measures include:

- Direct oversight by the NO/MLRO of all customer due diligence (CDD) activities undertaken by the Firm.
- Electronic identity verification through CreditSafe.
- Electronic verification checks for politically exposed persons and sanctions checks.

- Adverse media searches to identify and assess relevant publicly available information.
- Access to an external AML compliance consultant for specialist advice and guidance.

The risk summaries below are drawn from the Firm's most recent Firm-Wide Risk Assessment (FWRA), which contains a more detailed analysis of the risks identified and the controls applied to mitigate them.

Firm-Wide Risk Assessment

Purpose

The Firm-Wide Risk Assessment (FWRA) is a core component of our Anti-Money Laundering (AML) compliance framework. It ensures that money laundering and terrorist financing risks relevant to the business are identified, evaluated, and mitigated in accordance with UK regulatory requirements.

Scope

This policy applies to all business areas, employees, and transactions undertaken by the firm. It covers both current and emerging risks that may arise from our business processes, client base, and transaction types.

Policy Statement

The FWRA takes into account:

- Risks identified since the previous annual assessment; and
- Risks anticipated in relation to our business model, typical clients, and standard transaction patterns.

It is the policy of this firm to:

- Conduct periodic reviews of the FWRA to ensure it remains accurate and reflective of our operational and regulatory environment.
- Apply timely updates whenever there is a change in risk profile, business activities, or legal requirements.
- Maintain FWRA records under the supervision of the NO/MLRO, while ensuring access is available to all staff for reference and guidance.

Risk Categories Considered

In line with UK Government guidance, our FWRA assesses risk across five key categories:

- Client/Customer Risk
- Transaction Risk
- Service/Product Risk
- Delivery Channel Risk
- Geographic Risk

Approach to Risk Mitigation

Our risk mitigation measures are proportionate to the size, scale, and nature of our business. This proportionate approach enables the Firm to:

- Achieve its growth objectives;
- Maintain a safe and compliant working environment for employees; and
- Ensure full adherence to applicable AML legislation.

Key features of our approach include systematic risk identification and assessment by applying structured processes to identify and evaluate risks in each of the five defined categories. Which includes targeted, risk-based controls and procedures. We do this by:

- Implementing proportionate mitigation measures aligned to the assessed level of risk.
- Applying Enhanced Due Diligence (EDD) where high-risk indicators are identified.
- Ongoing monitoring of transactions and relationships to detect suspicious activity.
- Providing regular AML training so staff can identify, escalate, and address risks effectively.

Risk on a Case-by-Case Basis

In addition to conducting an annual Firm-Wide Risk Assessment, the firm assesses risks on a case-by-case basis as they arise. Ongoing risk management is achieved through the application of control procedures, including the appropriate level of Customer Due Diligence (CDD), whether simplified, standard, or enhanced, as set out in **Chapter Four** of this policy.

It is the policy of the firm that all staff remain vigilant and exercise professional judgement when applying the established risk-based criteria and rules. Any doubt, concern, or suspicion

regarding a perceived, attempted, or actual breach of AML legislation must be reported to the NO/MLRO at the earliest reasonable opportunity.

Identification of 'Red Flags'

The identification of "Red Flags" is a critical element in detecting potential money laundering or breaches of applicable AML legislation. Red Flags frequently provide the basis for forming suspicion or knowledge that such activity may be occurring. To identify Red Flags effectively, staff are required to conduct comprehensive AML checks and apply a proportionate, risk-based approach, taking into account any indicators identified before, during, or after a transaction. This approach relies on a strong level of understanding developed through structured training, practical experience, the use of online verification tools, and the provision of adequate supervision.

Chapter 3 - SYSTEMS AND CONTROLS

The firm's policies, controls, and risk assessment procedures are designed to be fully consistent with the Money Laundering Regulations and the most recent government guidance. These measures, described in this manual and further supported by the Reference Guide, ensure that the business operates in full compliance with its legal and regulatory obligations.

- **Customer Identification and Verification** – The firm undertakes rigorous verification of the identity of all persons conducting business with us, obtaining and recording sufficient information to "know its customer" and to understand and anticipate the expected pattern of business.
- **Reporting Suspicious Activity** – Employees must report any suspicious activity to the NO/MLRO or another authorised individual with delegated responsibility. This obligation includes situations where a potential new business relationship is declined due to suspicion of criminal conduct.
- **MLRO Review of Internal Reports** – The NO/MLRO will review all internal reports in light of the information available and determine whether they give rise to knowledge, suspicion, or reasonable grounds to suspect money laundering or breaches of AML laws.
- **Ongoing Monitoring of Business Relationships** – All business relationships are monitored regularly to ensure they remain consistent with the customer's known profile, with particular attention to large or unusual transactions, higher-risk activities, and long-term arrangements such as off-plan purchases or commercial rentals.
- **Record Keeping** – Records are maintained to provide a complete audit trail for the statutory retention period of five years.
- **Cooperation with Authorities** – The firm will cooperate fully with relevant reporting and investigative authorities to the extent required by law and regulation, and in a manner that does not breach client confidentiality.
- **Customer Due Diligence** – CDD, whether simplified, standard, or enhanced, will be conducted as appropriate, and determinations will be made regarding whether a customer is a Politically Exposed Person (PEP) or is subject to adverse media or sanctions. Each client and transaction will be assigned a risk rating of low, medium, or high.

- **Internal and External Assessments** – The firm will retain detailed records of all regular internal and external assessments or audits of our systems and controls to ensure their continued effectiveness and compliance with the Money Laundering Regulations. Where weaknesses are identified, the remedial actions taken will be documented and retained in our compliance records.

The NO/MLRO has overall responsibility for ensuring that the firm's anti-money laundering (AML) policies, controls, and procedures (PCPs) are effective, proportionate, and compliant with the Money Laundering Regulations 2017 (MLR 2017), the Proceeds of Crime Act 2002 (POCA), and other applicable legislation.

The NO/MLRO duties include, but are not limited to:

- **Oversight of AML Framework:** Ensuring that the firm's AML PCPs are appropriately designed, implemented, and maintained, and that they reflect the size, scale, and complexity of the business. This includes regular evaluation of their effectiveness and the prompt implementation of necessary improvements.
- **Firm-Wide Risk Assessment:** Overseeing the preparation, maintenance, and regular review of the Firm-Wide Risk Assessment (FWRA), ensuring it is accurate, up-to-date, and responsive to changes in the business or regulatory environment.
- **Governance and Reporting:** Providing regular AML compliance reports to the Board or equivalent governing body, highlighting risk exposures, compliance performance, audit results, and remedial actions. Ensuring AML considerations are integrated into strategic business decisions.
- **Policy Development and Review:** Ensuring that the firm's AML policies and procedures are reviewed and updated at least annually, or more frequently as required by regulatory changes or business developments.
- **Training Oversight:** Overseeing the delivery of AML training across the firm, ensuring that it is role-specific, regularly refreshed, and that completion is properly recorded. Evaluating the effectiveness of training through assessment and monitoring.
- **Compliance Monitoring and Audit:** Implementing a compliance monitoring programme, coordinating internal and/or external audits, and ensuring that audit recommendations are addressed and implemented promptly.

- **Regulatory Liaison:** Acting as the primary point of contact with HMRC and other relevant authorities for AML supervision, inspections, and inquiries, and ensuring that all regulatory communications are managed appropriately.
- **Record-Keeping:** Ensuring that AML-related records, including CDD/EDD files, training logs, internal audit reports, and SAR records, are maintained in accordance with the statutory retention period and are accessible for inspection.
- **Promoting a Compliance Culture:** Fostering an organisational culture where AML compliance is viewed as integral to ethical business practice, encouraging staff to take personal responsibility for identifying and reporting suspicious activity.

The NO/MLRO role is fundamental to maintaining the integrity of the firm's AML framework and ensuring ongoing compliance with legal and regulatory obligations. This position carries a high level of accountability and requires the individual to act with independence, authority, and professional diligence at all times.

Chapter 4 – CUSTOMER DUE DILIGENCE

Where appropriate, the firm applies varying levels of Customer Due Diligence (CDD) in accordance with a risk-based approach. The three recognised levels of CDD, Simplified Due Diligence (SDD), Standard Due Diligence (CDD), and Enhanced Due Diligence (EDD), are summarised, along with a more detailed explanation provided in the Reference Guide.

If CDD measures are delayed or prove inadequate, the transaction must be suspended without exception, and the matter reported immediately to the NO/MLRO. Additional guidance on identifying and managing delayed or inadequate CDD is also provided in the Reference Guide.

Undertaking and timing of CDD

This firm completes CDD at the earliest appropriate stage of any transaction or business relationship. For sellers, we undertake CDD when we receive a formal instruction to market a property. For buyers, we conduct CDD when an offer to purchase has been formally accepted by the seller. For ongoing business relationships with landlords or tenants, we refresh CDD at appropriate intervals, with the frequency determined by the assessed level of risk. We refresh CDD more frequently where there are changes to a client's circumstances, such as alterations in beneficial ownership, changes of address, changes of bank account, or replacement of occupiers. If we have any doubts about the accuracy, completeness, or validity of previously obtained identification information, we repeat the CDD process immediately. Where we know or suspect money laundering, terrorist financing, or have reasonable grounds to doubt the authenticity of documentation or information, we apply Enhanced Due Diligence without delay.

- We complete verification before any marketing activity begins, before an offer is formally accepted, or before continuing an existing client relationship. We do not accept funds or enter into contractual obligations until we have fully verified the client's identity.
- We document all CDD checks, including the date of verification, the documents reviewed, the verification method used, and any additional checks performed. We retain these records in accordance with our record-keeping policy and legal requirements.

We apply a risk-based approach at all times. Clients assessed as higher risk, including those located in higher risk overseas locations, politically exposed persons (PEPs), those with adverse media or those with overly complex company trust structures, professional enablers, loans, trusts, special purpose vehicles (SPV's), underground banking, the sale or purchase of multiple properties and Real Estate Investment Trusts (REITs) undergo more frequent and rigorous verification measures by giving consideration to applying enhanced due diligence.

The table below provides an overview of these risks and can be used to support a risk-based approach.

This table is intended as a reference guide only and is not limited to the risk listed.

Risk Area	Risk	Common indicators	Risk Level
Residential property laundering	Using any-value homes to clean funds; buyer affordability doesn't match property	Income/wealth mismatch, rapid flips, multiple properties at once	High ML exposure; harder to spot vs commercial
Commercial property laundering	Premises used for cash-based crime or as fronts	Cash-intensive businesses; opaque companies; cannabis grows; trafficking links	High ML & predicate offences
Super-prime property **£5m London & SE** **£1m rest of UK**	High-value assets used to store/park illicit wealth	PEP involvement; complex structures; prestige purchases	High ML/PEP exposure
Customer profile & behavior	Client circumstances do not fit transaction	Secretive/evasive; won't share CDD/SoF/SoW; unusual agent choice; odd patterns	Elevated ML/TF, potential fraud
Multiple transactions/patterns	Repeated sales or multiple properties to layer funds	Same asset traded often; unexplained value swings; many intermediaries/solicitors	Layering/red flags obscured across counterparties
Unusual pricing	Above/below market values without rationale	Asking price far off valuation; overpayments/refunds	Placement/layering via value transfer
Complex or unusual corporate structures	Opaque ownership/control to hide beneficial owners	Many layers; shells; offshore arms; nominee roles	BO concealment; sanctions/PEP exposure
Non-transparent legal entities	Vehicles designed to disguise BO/flows	SPVs, PIVs, bearer share features, poor registries	High ML risk via anonymity
Corporate structures not wholly UK-based	Multijurisdictional chains complicate tracing	Overseas affiliates; portions in secrecy hubs	Ownership tracing & SoF complexity
Intermediaries	Distance between client and EAB for anonymity	Excessive middlemen; 'anonymity services' marketing	Harder KYC; higher ML risk

The NO/MLRO monitors the escalation of CDD to enhanced status especially for any existing clients for which ongoing monitoring is applicable. CDD is generally a cumulative process with more than one document or data source being required to verify all of the necessary components. A list of the identification documents or data that can be used for CDD purposes can be found within the Reference Guide.

Standard CDD

Standard CDD is the most common form of due diligence we undertake in our estate agency business. It ensures that we meet our legal obligations under the Money Laundering Regulations 2017 and that we have a clear understanding of who we are dealing with before progressing any transaction.

Our Standard CDD process involves four key steps:

- **Identifying the Customer and Gathering Information**
  We collect sufficient information to clearly identify our customer. For individual clients, this includes their full name, date of birth, residential address, and contact details. For corporate clients, we obtain the registered company name, registration number, registered office address, trading address (if different), and the details of directors and beneficial owners. In cases involving trusts, we identify the trustees, settlors, and any beneficiaries.
- **Verifying the Customer's Identity**
  We verify the identity information provided using reliable, independent sources. This may include original documents, certified copies, or electronic verification systems. For individuals, this typically involves reviewing a current passport, photocard driving licence, or other government-issued identification, together with recent proof of address such as a utility bill or bank statement. For companies, verification may involve checking Companies House records, obtaining a Certificate of Incorporation, and confirming the identities of persons with significant control (PSCs).
- **Understanding the Proof and/or Source of Funds**
  We establish and clearly document how the client intends to pay for the transaction or rent and where necessary identify the origin of those funds. This process includes reviewing supporting evidence such as recent bank statements, completion

statements provided by solicitors, investment portfolio statements, or other relevant financial documentation. We assess whether the source of funds is reasonable and consistent with the customer's declared occupation, financial position, and the scale of the transaction. Where the information provided is incomplete, unclear, or inconsistent with the customer's profile, we conduct further enquiries and request additional evidence to ensure the source of funds is fully understood and verified before proceeding.

- **Understanding the Purpose of the Transaction**
  We record the intended purpose and nature of the transaction. For example, we determine whether the customer is purchasing as an investment, or on behalf of another party. We consider whether the stated purpose aligns with our knowledge of the customer and whether it presents any unusual or higher-risk characteristics.

The actual level of CDD completed, together with copies of the evidence obtained, is recorded in our compliance files. Where risks or concerns are identified, we may escalate the matter to Enhanced Due Diligence (EDD) procedures. In low-risk cases, we may apply Simplified Due Diligence (SDD), subject to regulatory conditions. Both EDD and SDD are explained in detail later in this chapter.

Identify the Customer

Every member of the Firm makes it clear to customers that we are legally required to carry out Customer Due Diligence (CDD) on all clients. This requirement is also set out in our terms of business to ensure transparency from the outset. This ensures that customers are aware of our statutory obligations and fully understand the reason for any requests for personal information or documentation.

To determine which individuals and legal entities in a transaction chain require CDD, we first identify the "customer." This involves establishing ownership of the property or land involved, or identifying the paying party for our services, for example, the buyer or the person on whose behalf we are providing estate agency services. There may be one or more customers in a single transaction, on either the buying or selling side, including counterparties with whom we have a direct business relationship.

Once we have identified the customer or customers, we must determine whether they are a natural person or a legal entity. The type of entity involved will dictate the level and nature of CDD required, as set out in the relevant sections of this policy.

Following identification, we proceed with the next stage of the CDD process by obtaining documentary and/or electronic evidence of the customer's identity. This may include certified copies of official documents, information from reputable online sources, or other verification methods that meet regulatory standards.

Verification of Customer ID

There are several ways to verify a person's identity. HMT Guidance includes the following acceptable methods:

- Obtaining or viewing original documents and ensuring that they are valid and genuine, by comparing them to published, authoritative guidance that outlines security features the EAB can then certify copies of these original documents by stating that they are 'copies of original documents as seen by me and are a true likeness of the client met face to face' the certification must be signed and dated.
- Where the client has been seen face to face, comparing the likeness of the person to the document is important.
- Conducting electronic verification that properly establishes the customer's identity, by using document fraud checks, biometric facial comparison and liveness checks.
- Obtaining information from another regulated party operating within a regulated sector i.e. a solicitor that can be used in conjunction with other documents and information to prove a customer's legitimacy.
- If a client cannot be met in person, we request a copy of an appropriate identification document that has been certified by a regulated entity or individual, in line with the criteria outlined above. We then verify the credentials of the certifying party by checking with the relevant supervisory body to ensure they are suitably qualified to certify documents. For example, for a legal professional in the UK, we confirm their registration via the Law Society or Solicitors Regulation Authority (SRA) website.

Third Party Representatives

When a client is represented by a third party, our employees conducting CDD will fully understand the nature and scope of the relationship between the third party and the client. Written authority confirming that the third party is authorised to act on the client's behalf must be obtained before proceeding. In such cases, we verify the identity of both the third party (unless regulated or acting as a personal assistant) and the underlying client. This involves collecting and verifying appropriate documentation for each, in accordance with the CDD requirements set out in this policy.

Legal Entities & Legal Arrangements

We always establish the beneficial owner or ultimate beneficial owner (UBO) of any Firm or trust involved in a transaction. This requires obtaining and reviewing the Firm's registration documents or the deed of trust, together with all other relevant documentation needed to confirm ownership. We also identify any person with significant control (PSC), in accordance with the definitions set out in the Reference Guide. The register of members (share register) is a key source of information for identifying the UBO or PSC of a legal entity. Once the beneficial owner has been established, we verify their identity using the same procedures and standards applied to individual clients, ensuring full compliance with our CDD requirements.

Proof / Source of Funds

As outlined in the previous section, proof and/or source of funds refers to the means and origins of the money being used to finance a purchase. We always establish how the client intends to fund the transaction and from where those funds will originate.

For commercial properties, higher-value transactions (usually those in the top 5% of commercial properties in the relevant area), we apply Enhanced Due Diligence (EDD) as standard.

If at any stage during the CDD process a red flag is identified, we escalate the case from standard CDD to Enhanced Due Diligence. This may include additional checks to establish the source of funds (SOF) and, where appropriate, the source of wealth (SOW). Further guidance on EDD and SOW is provided later in this policy.

Enhanced Due Diligence

Where there are doubts, concerns, red flags or suspicions about a client, the parties to a transaction, or the nature of the transaction itself, Enhanced Due Diligence (EDD) may be required. In such cases, the MLRO/NO is be informed. EDD is mandatory whenever any of the following circumstances apply:

- Politically Exposed Persons (PEPs), including their family members or close associates, are involved in the transaction.
- The transaction involves high-risk countries known to have weak anti-money laundering (AML) controls or high levels of corruption.
- The client has provided false, altered, or stolen identification documents.
- The transaction is unusually complex, lacks a clear economic rationale, or is unusually large given the client's profile.
- For commercial properties, higher-value transactions (usually those in the top 5% of commercial properties in the relevant area).
- There is a high risk of money laundering, or information becomes available from the authorities or other credible sources, for example, adverse media reports or open-source intelligence.
- The client is a sanctioned individual or entity or is closely linked to a sanctioned individual or organisation, including through family, business, or other associations.

Enhanced Due Diligence (EDD) requires additional verification measures, the collection of further documentation, and more detailed checks to address the higher level of risk identified. In addition to the standard CDD steps, EDD includes establishing the source of funds, meaning the origin of the money used for the transaction, and in some cases, also requires an assessment of the source of wealth. When reviewing source of wealth, we consider factors such as income from employment, business ownership, investments, inheritance, or the sale of assets. We assess whether the declared wealth is consistent with the client's age, profession, lifestyle, and the size of the transaction. Where necessary, we request credible and independent documentation to substantiate the explanation provided. To support this process, we also require the client to complete a self-declaration form.

At the discretion of the NO/MLRO, EDD measures may also include:

- Requesting additional client information, including steps to verify the CDD already obtained,
- Requesting clarity on the purpose of the transaction, the source of funding or source of wealth
- Clarifying any confusion around the nature of the business relationship
- Frequent reviews of the business relationship, as well as in-person meetings with the client or other ongoing monitoring procedures

If satisfactory EDD is not obtained, the transaction should not be concluded and the NO/MLRO should consider making a disclosure to the relevant authority.

Simplified Due Diligence

Where the risk of money laundering is assessed as extremely low, and specific circumstances apply, we may apply Simplified Due Diligence (SDD). An example of when this may be appropriate is where the client operates within another regulated sector that is subject to equivalent AML standards.

Before applying SDD, we must confirm that the client is eligible. This may include checking Firm registers, confirming the Firm's listing on a regulated entity register (such as the FCA, HMRC, or SRA), or verifying its status through other reliable sources. For any corporate client, we must obtain the full business name, Firm registration number, country of incorporation, and the full registered address.

In applying SDD, we confirm the client's existence through appropriate Firm documentation obtained and supported by verification through Companies House (for UK entities), open-source checks, and confirmation that the client itself is a regulated entity. Reference Materials provide further detail on verifying different types of organisations.

It is also essential to confirm that the individual providing instructions on behalf of the client has the proper authority to do so, and in some circumstances, we may also verify the identity of that individual.

If we determine that SDD is appropriate, we must record the decision-making process, along with copies of all documentation reviewed in support of the decision. SDD cannot be applied where we are relying on another estate agency business (EAB) to perform due diligence, nor can it be applied in any situation where Enhanced Due Diligence (EDD) is required.

Sanctions

As a relevant firm, we are fully aware of the UK financial sanctions regime and the reporting obligations that apply to us under this framework.

In line with these obligations, we recognise that we must report to the Office of Financial Sanctions Implementation (OFSI) as soon as practicable if, during the normal course of our business, we know or have reasonable cause to suspect that a person:

- is a designated person;
- has committed a breach of financial sanctions regulations; and/or
- is a customer of the firm and, in such circumstances, we must also report to OFSI the nature and amount or quantity of any funds or economic resources held for that customer at the time the knowledge or suspicion first arose.

When making a report to OFSI under the sanctions reporting obligations, we will ensure that it includes:

- the information or other matter on which our knowledge or suspicion is based;
- any details we hold about the individual or designated person that may assist in confirming their identity; and
- where applicable, the nature and amount or quantity of any funds or economic resources we hold for a designated customer.

This process ensures that we remain compliant with the UK financial sanctions regime, uphold our regulatory obligations, and support the wider objective of protecting the financial system from abuse.

CDD Risk Assessment

In the context of money laundering, there are a number of potential "red flags" that must be carefully assessed during the Customer Due Diligence (CDD) process. These indicators of risk may arise individually or in combination, and each must be considered in light of the wider circumstances of the transaction. This Firm recognises that certain factors present heightened risk in property transactions and will assess them on a case-by-case basis. Where such concerns are identified, the CDD file may be referred to the NO/MLRO who will then review the file in full, taking all relevant matters into account before determining the appropriate course of action.

Customer Risk

- A customer provides only copies of ID documents rather than originals.
- Unexplained delays in providing requested verification documents for a transaction.
- An entity cannot be located or verified through online presence or public records.
- The use of an alias or unusual secrecy regarding personal information.
- Reliance on a P.O. Box or non-standard address instead of a verifiable residential or business address.
- Refusal or reluctance to provide requested information, particularly relating to financial details, preventing the progression of the transaction.
- Unwillingness to meet in person without a valid explanation.
- Inability to identify the beneficial owner or controlling party of a Firm.
- The client is known to have convictions, is under investigation for acquisitive crime, or has known criminal associates.
- Use of intermediaries or representatives without a clear or legitimate reason.
- The customer is a Politically Exposed Person (PEP).
- The customer is a family member or close associate of a PEP.
- Reluctance to disclose proof or source of funds, particularly when accompanied by threats to withdraw from the transaction.

Transaction Risks

- Unusual sales, purchase or lettings activity that is inconsistent with the client's known means or prior behaviour.
- Third-party payments that do not match the named tenant or permitted occupier.
- Transactions involving super-prime property, defined as those valued above £5m in London and the South-East or above £1m throughout the rest of the UK.
- Reliance on a counterparty to complete a purchase or rental transaction.
- Payments made in cash or cryptocurrency.
- Use of complex, opaque, or layered Firm structures.
- Property values that appear disproportionate to the client's profile or financial position.
- Multiple smaller payments made in an attempt to avoid threshold limits.
- Clients pressing for unusual urgency or speed in completing the transaction.
- Properties being resold or "flipped" quickly at significantly higher values, multiple properties, unusual pricing.
- Cash gifts from third parties where the gifter appears to have low or inconsistent income.
- Requests for deposits to be refunded without a clear intention to proceed with the property purchase.
- Adverse information identified through open-source checks, such as negative media coverage, director disqualification, convictions for dishonesty, or association with bribery or corruption.

Geographic

- This business faces a higher risk as we are dealing with a client base and location with high-net-worth individuals in metropolitan areas
- The customer is resident in, or has connections to, a jurisdiction with weak or non-existent AML controls, or where corruption levels are high.
- The transaction involves a country where underground or parallel banking systems are a common business practice.
- The transaction is linked to a jurisdiction known for highly secretive banking practices or opaque corporate law.
- The transaction involves, or has connections to, a country that is subject to international sanctions or has ties to sanctioned jurisdictions.

- The customer makes unusual use of offshore accounts, companies, or other structures that appear inconsistent with their instructions or profile.

Delivery Channels

- Certain delivery channels present a higher risk than others, particularly when clients are dealt with online and there is no face-to-face contact.
- The business may be especially vulnerable when a high proportion of clients are connected to higher-risk overseas jurisdictions. In such cases, it can be more challenging to verify the beneficial owners of overseas entities and to establish the source of offshore funds.
- Cross-jurisdictional factors such as language barriers, identity verification challenges, and differing legal frameworks can increase complexity and create opportunities for money laundering.

Registration of Sub/Joint Agent/Property Finder

In line with HMRC guidance, it is this Firm's policy to confirm whether any estate agency business (EAB) with which we are dealing is registered with HMRC. We do not rely on Customer Due Diligence (CDD) material provided by an unregistered UK EAB. In such cases, we will establish direct contact with the client and obtain full CDD ourselves.

Where we identify that an EAB is not registered, or has not yet applied for registration, we will escalate the matter to the NO/MLRO as soon as practicable. The NO/MLRO will then determine whether a report to the relevant authority is required.

Understanding Risks and taking action

In line with HMRC guidance, the Firm should remain aware of geographical risk, which includes FATF grey and blacklisted countries as well as several other jurisdictions identified with specific risk factors. A list of these countries along with the associated risk can be found below:

Jurisdiction / Country Group	Specific Risks Identified	Typology / Context
Russia (specific to sanctions exposure)	Sanctions (ML/TF, proliferation financing), corruption risk	Super-prime property, sanctioned oligarchs
Russia, Ukraine, China, Pakistan, Angola, Ghana, Nigeria	High-value foreign buyers using illicit funds from corruption, fraud, organised crime	Super-prime property transactions, residential & commercial laundering
Eurasia (Belarus, Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan, Caucasus incl. Azerbaijan, Georgia, Armenia)	Predicate offences (corruption, fraud) routed through UK property	Super-prime transactions, opaque ownership
British Virgin Islands (BVI), Gibraltar, Guernsey, Jersey, Liechtenstein, Luxembourg, USA, Hong Kong	Offshore/secrecy jurisdictions used to obscure beneficial ownership	Trusts, SPVs, PIVs, corporate layering
London & Southeast (Super-prime ≥£5m)	Concentrated hub for foreign investment, high exposure to PEPs, secrecy structures	Super-prime property laundering & prestige purchases
Scotland (Super-prime ≥£1m)	Attractive to foreign buyers, exposure to illicit funds	High-end property transactions
Western Balkans (incl. Albania)	Lettings-linked organised crime groups; corruption and drug trafficking proceeds	Lettings, residential buy-to-let, commercial laundering (including under threshold cash based)
Afghanistan	Conflict, terrorist financing, corruption, weak AML regime	HRTC/terrorist financing
Middle East (regional risk)	Terrorist financing, corruption, conflict zones, sanctions	TF & proliferation financing
Colombia	Drugs trafficking proceeds laundered into UK/overseas property	Predicate offences ML laundering
Dubai / UAE	Secrecy jurisdiction, high-value property hub, links to ML/TF	Offshore property & corporate ownership
Singapore	Secrecy jurisdiction, financial centre risk, potential illicit fund flows	Offshore investment into UK real estate
Turkey	Corruption, sanctions circumvention, regional organised crime	Property & commercial laundering

Jurisdiction / Country Group	Specific Risks Identified	Typology / Context
Syria	Terrorist financing, proliferation financing, sanctions	Sanctioned regime
Countries with high geographical terrorism risk (Middle East, conflict regions)	Concealment of beneficial ownership & high risk of the extraction of funds (leaving the country)	Broader overseas jurisdiction risk indicators
All jurisdictions under Increased Monitoring (FATF grey list)	Weak or developing AML/CTF frameworks	Elevated due diligence required but not always high risk
High Risk Countries (FATF blacklist)	Strategic deficiencies in AML/CTF regimes	High ML/TF/Proliferation risk, EDD mandatory
Iran	Proliferation financing, Terrorist financing	Sanctioned regime
Myanmar	Terrorist financing, proliferation financing, sanctions	Sanctioned regime
North Korea	Proliferation financing, weapons programmes	Sanctioned regime

Relying on a Third Party to Conduct CDD - MLR 39 [Reliance 39]

This Firm may, on occasion, rely on Customer Due Diligence (CDD) carried out by another regulated entity, as permitted under Regulation 39 of the Money Laundering Regulations. However, it is important to note that where reliance is placed, this Firm remains fully liable for any errors or omissions in the CDD performed by the third party we understand that reliance does not extend to enhanced due diligence checks for customers deemed to be high risk.

As a matter of practice, we ordinarily conduct our own CDD. Reliance on a counterparty is only considered where it is deemed practical and appropriate, and only where we are satisfied that the third party has undertaken CDD to a standard that fully complies with the Money Laundering Regulations and the client's documentation is always requested.

If there are any doubts or concerns regarding the adequacy of the CDD carried out by a third party, we will, wherever reasonably practicable, conduct our own CDD. In such cases, we will maintain clear records of all attempts made to obtain the relevant documentation and evidence supporting our decision-making process.

Authorisation and Conditions for Reliance (Regulation 39)

Only the Nominated Officer (NO) or Money Laundering Reporting Officer (MLRO) may authorise the use of Regulation 39 reliance on another regulated entity. Reliance under Regulation 39 requires that specific conditions are agreed in writing, which we normally confirm by email. The detailed requirements are set out in the Reference Materials. Where the Firm requests reliance CDD from another party and that party refuses to provide it, we will document all attempts made to obtain the CDD and retain these records for audit purposes.

It is important to note that if a third party or intermediary representing the client provides us with their client's CDD documentation, this does not constitute "reliance" under Regulation 39 of the Money Laundering Regulations. In such cases, the responsibility for CDD remains with this Firm. For customers who are subject to Enhanced Due Diligence (EDD), enhanced monitoring is mandatory. This includes ongoing scrutiny of transactions and the application of all procedures set out in this policy, which must be followed at all times.

Chapter 5 – RECORD KEEPING, DATA PROTECTION AND TRAINING

Record Keeping

Every employee has a responsibility to ensure complete and accurate record keeping in support of our Anti-Money Laundering (AML) programme.

All documents and information generated during the Customer Due Diligence (CDD) process is retained separately from routine client sale, purchase, or memorandum files. These records are stored securely and in compliance with our obligations under the UK General Data Protection Regulation (GDPR).

AML records must be retained for **five years** from the date a business relationship ends or from the completion of a transaction. Where a transaction is subject to an ongoing investigation, or another supervisory authority requires access to the records, the Firm will retain them until formal confirmation has been received that they are no longer required.

The Firm maintains AML records across the following categories:

- CDD documentation, including client identification, transaction details, and records of our risk-based approach and decision making.
- Internal and external reports of suspicion or knowledge of money laundering, including details of investigations, the basis for suspicion, and any matters not pursued.
- Training records, including details of training provided, updates on AML laws and compliance monitoring, training dates, and attendance registers.
- The firm wide risk assessment, along with our AML policies, controls, and procedures.
- Agreements with third party CDD service providers or outsourced compliance providers.
- Reports prepared by the NO/MLRO.

Upon expiry of the statutory five-year period, it is the Firm's policy to delete personal data unless one of the following applies:

- Retention is required by law or for the purposes of ongoing court proceedings.
- There are reasonable grounds to believe the records are still needed for prospective legal proceedings.
- The data subject has expressly consented to their continued retention.

Data Protection & GDPR

The Firm is fully committed to meeting all legal and regulatory requirements in respect of record keeping. In line with Regulation 40 of the Money Laundering Regulations, the NO/MLRO have established a system for securely storing all documents and information obtained to satisfy AML and CDD obligations. These records are kept separately from routine client files to ensure confidentiality and integrity. Any personal data obtained by the Firm is processed solely for the purposes of preventing money laundering and terrorist financing, or where its use is otherwise permitted under applicable legislation, or with the explicit consent of the data subject.

It is strictly against Firm policy, and against the law, to use any personal data gathered through AML processes for competitive, commercial, or non-compliance purposes.

Training

Relevant members of staff receive regular, high-quality, bespoke training tailored to their role. As firm wide risk assessments are updated annually, it is our policy that staff undertake training on a regular basis, and at least once every two years, unless changes in legislation, regulation, or our business activities require training to be delivered more frequently.

New members of staff receive formal AML training as soon as practicable after their appointment. Similarly, existing staff whose roles or responsibilities change receive additional training as soon as possible after those changes take effect.

Senior Management and the NO/MLRO may also require training to be tailored from time to time to meet the particular needs of the business.

We maintain full records of all training undertaken. These records include the employee's name, the date of the training, the training provider, and the content delivered.

The NO/MLRO is responsible for ensuring the provision of up-to-date resources and training materials to support the implementation of this policy. All staff have access to these resources, and further detail on our approach to training can be found in the Reference Guide together with a sample training log.

Chapter 6 - ANTI-BRIBERY & CORRUPTION

It is the Firm's policy to conduct all business honestly, ethically, and in full compliance with UK law relating to the prevention of bribery and corruption. The Firm is bound by the Bribery Act 2010 in respect of its activities both in the UK and overseas.

In line with this commitment, the Firm may, where appropriate:

- Limit corporate hospitality to events with a clear and proportionate commercial rationale.
- The giving or receipt of cash gifts or cash equivalents (e.g., vouchers) is not allowed.
- Modest and reasonable gifts or hospitality may be acceptable if they are clearly for legitimate business purposes, proportionate, and properly recorded.

We adopt a zero-tolerance approach to bribery and corruption. We are committed to acting with professionalism, fairness, and integrity in all our business dealings and relationships, and to implementing and enforcing robust systems to counter bribery. The prevention, detection, and reporting of bribery or corruption are responsibilities shared by all employees and individuals acting on behalf of the Firm.

Staff Anti-Bribery Responsibilities

All employees are required to avoid any activity that might lead to, or suggest, a breach of this policy. Any advantages given or received must be kept to a minimum, and a record must be created. Receipts detailing the amount and reason must be attached and retained. All employees are responsible for preventing, detecting, and reporting to the NO/ MLRO as soon as possible any suspicion or knowledge of bribery or corruption.

Staff must notify the NO/MLRO as soon as is reasonably practicable if they believe, know, or suspect that:

- a conflict with this policy has occurred, or
- a conflict may occur in the future.

Any employee who breaches this policy will face a disciplinary review, which may result in dismissal for gross misconduct. If a staff member is a victim of bribery or corruption, they must notify the NO/MLRO or a member of Senior Management as soon as possible.

Chapter 7 - SUSPICIOUS ACTIVITY REPORTING PROCEDURE

A Suspicious Activity Report (SAR) is a disclosure made to the National Crime Agency (NCA) concerning known or suspected money laundering under Part 7 of the *Proceeds of Crime Act 2002 (POCA)* or terrorist financing under Part 3 of the *Terrorism Act 2000 (TACT)*.

Once a member of staff forms a suspicion, has knowledge, or has reasonable grounds to suspect or know that a person is engaged in money laundering or terrorist financing in relation to any transaction with which the firm is involved, they must notify the NO/MLRO as soon as reasonably practicable. An initial oral notification may be given, but this must always be followed by a written internal report. A standard form for making this type of report is available in the Reference Guide.

Upon receiving an internal report, the NO/MLRO will carry out a written evaluation. This evaluation should record the nature of the report received, the reasons for it, the internal and external Customer Due Diligence (CDD) information that has been obtained and considered, and any discussions with colleagues. It must also document the decision taken and the reasons for the course of action pursued. The evaluation record should be maintained whether or not a SAR is submitted to the NCA. If a SAR is submitted, it must be kept together with the internal report.

Before deciding to make a SAR, the NO/MLRO will conduct their own investigation into the information provided. This may involve verifying the CDD already obtained and gathering further information to assist in determining whether a report should be submitted. Any decision to submit a SAR to the NCA should be made by the NO/MLRO in consultation with a member of senior management. The reasoning for filing, or deciding not to file, a SAR must always be documented on the client's anti-money laundering file. After a SAR has been filed with the NCA, no further Customer Due Diligence checks should be made directly with the subject of the report, in order to avoid the risk of committing a "tipping off" offence. Further guidance is available in the Reference Guide.

The NO/MLRO is also responsible for ensuring that internal reports and external SARs are taken into account in the firm's annual written risk assessment and that regular reports on the firm's money laundering and terrorist financing risk profile are made to senior management. All communication with the NCA, including requests for further information or the service of court

orders, must be handled directly by the NO/MLRO. Staff should refer to the firm's Guidance Document for more information regarding SAR requirements and procedures.