ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM COMPLIANCE POLICY

All references in this policy to money laundering include terrorist financing, and references to anti-money laundering ('AML') include countering the financing of terrorism ('CFT').

The contents of this policy have been approved by the Directors of the firm. It is important that you read and apply it.

1. Purpose and Scope

Purpose

This policy sets out the firm's procedures to prevent money laundering and terrorist financing. It explains what you must do to comply with the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 as amended ('MLR'), the Proceeds of Crime Act 2002 ('POCA'), and the Terrorism Act 2000.

This policy should be read in conjunction with the firm's Equality, Diversity and Inclusion Policy.

Scope

This policy applies to all directors, solicitors, fee earners, support staff, temporary employees, agency staff, consultants and contractors, wherever they may be based.

The MLR apply only to certain types of regulated work. However, **the procedures set out in this policy must be applied to all clients and all matters**.

Your main obligations are to:

- Carry out customer due diligence and ongoing monitoring, including source of funds and source of wealth checks
- Be familiar with this policy and the firm's AML procedures and ensure compliance
- Recognise and report suspicious circumstances to the MLRO
- Avoid tipping off a suspect about a report

WARNING
Failure to comply with the firm's anti-money laundering policies may be treated as gross misconduct and result in disciplinary action, which could ultimately lead to dismissal. Such failure may also put you at risk of prosecution under the Proceeds of Crime Act 2002 (POCA) and a significant fine from the SRA for economic crime offences.

2. Policy Statement

The firm is committed to full compliance with its obligations under the MLR and all associated AML and CFT legislation. We take a zero-tolerance approach to money laundering and terrorist financing. We have assessed the money laundering risks to which the firm is subject through our firm-wide risk assessment ('FWRA') and have implemented proportionate controls to manage those risks.

This policy reflects the FWRA and sets out the AML controls the firm has in place. The firm's assessment of the risks arising from its client base, services, geographic exposure, transaction types and delivery channels is set out in the FWRA. The controls in this policy are the firm's documented response to those assessed risks, as required by Regulation 19 MLR. It is reviewed at least quarterly and updated to reflect legislative changes, regulatory developments and the findings of internal audits and file reviews.

Under section 250 of the Crime and Policing Act 2026, the firm may be held criminally liable for an offence of this nature if it is committed by a senior manager acting within their actual or apparent authority, regardless of the firm's compliance systems. This applies in addition to the specific obligations set out in this policy.

3. Overview of Our Firm

Locations
Our office location is as follows:
St Giles Chambers, 14-16 Chapel Street, Cheadle, Staffordshire ST10 1DY

Number of employees
We have **17** employees. The breakdown across roles is as follows:

Directors: **3**
Fee earners: **5**
Support staff**: 9**

Practice areas
For the year ending **April 2026**, our practice areas were as follows**:**

45% Residential Conveyancing

22% Probate

11% Lasting Powers of Attorney

9% Matrimonial

6% Wills

4% Commercial Conveyancing

3% Other

Of those practice areas, the following involve AML regulated work:
Residential Conveyancing, Commercial Conveyancing & Probate matters Probate matters where we are managing the assets of the estate under instruction from the executors or as the executor.

AML regulated work makes up around **71**% of our overall work.

Plans to expand practice areas
We do not have plans to expand into other areas of AML regulated work.

Our clients
Our instructions come primarily from UK based private individual clients.

Our instructions typically come from:

- Repeat Instructions
- Recommendations from friends or family members that have used us previously
- Estate Agents
- Mortgage brokers
- Staff members or family and friends of staff members
- Review Solicitors Website

Our Geographical Area
Our client base is predominantly based in our geographical area, mainly individuals or families, local businesses and other organisations, most of whom are known to the firm and have been past clients. Around 85% of our clients are based in the Staffordshire area (and of those around half are based within a six-mile radius of our office).

We do, however, receive instructions from clients throughout the UK, particularly in conveyancing matters.

We do not have a client base with individuals or entities in high-risk jurisdictions, but this is confirmed at the outset and monitored as the matter progresses.

We are based in the United Kingdom, and the UK is a FATF registered country and is ranked as low risk on the Transparency International Corruptions Perception Index.

Our Products & Services

- Residential conveyancing; typically dealing acting for buyers/sellers or those wishing to remortgage their property.
- Commercial property; typically dealing with purchasing a business or dealing with the grant or assignment of business lease.
- Probate; typically dealing with the estate either just obtaining grant of probate or managing the assets of the estate under instruction from the executors or as the executor.
- Drafting Wills and/or Lasting Power of Attorneys
- Family; typically dealing with relationship breakdowns including divorces and finances.
- Employment; typically advising regarding settlement agreements.

The Types of Transactions we handle
In the year ending **April 2026,** we completed:

183 residential purchases

222 residential sales

35 commercial conveyancing matters

374 wills (approximately)

45 probate matters (approximately)

We do not tend to handle unusually large or complex transactions, those with unusual patterns or transactions without an apparent economic or legal purpose.

Our Delivery Channels
We deal with our clients in face-to-face meetings, telephone calls, in writing and by email. For all matters, including non-money laundering regulated work, we confirm the identity of the client (we use the Thirdfort verification platform to assist with this) and verify that the client is who they purport to be.

4. Policy Detail

Governance and nominated officers — Regulation 21(3) MLR

The MLR require the firm to appoint nominated officers with specific AML responsibilities.

- **Money Laundering Reporting Officer (MLRO): Timothy Halliday**

The MLRO is responsible for receiving and assessing internal suspicious activity reports, making external reports to the National Crime Agency ('NCA') where appropriate, and overseeing the day-to-day operation of this policy.

- **Deputy MLRO: Elizabeth Collins**

In the MLRO's absence, consult the deputy MLRO.

- **Money Laundering Compliance Officer (MLCO): Timothy Halliday**

The MLCO has overall responsibility for ensuring compliance with the MLR, maintaining written AML policies, controls and procedures ('PCPs'), overseeing training, and keeping records of all AML training and policy reviews. Questions about AML policies, internal systems and controls may be directed to the MLCO.

- **Compliance Officer for Legal Practice (COLP): Timothy Halliday**

The COLP has ultimate responsibility for all aspects of compliance within the firm.

If neither the MLRO nor the deputy MLRO is available, consult the MLCO or the COLP.

Policies, controls and procedures — Regulation 19 MLR

As required by Regulation 19 of the MLR, the firm maintains written PCPs to mitigate and manage the risks identified in the FWRA. Our PCPs are reviewed and updated regularly. We keep a written record of all changes and the steps taken to communicate them.

The firm's PCPs have been designed to address the specific risks identified in the FWRA across all risk categories, including client risk, geographic risk, product and service risk, transaction risk and delivery channel risk. Staff are required to apply the controls in this policy in response to those assessed risks.

The up-to-date copies of all internal policies can be found on the firms Intranet.

Internal controls — Regulation 21 MLR

Employee screening — Regulation 21(1)(b) and (2) MLR

All employees are subject to screening by way of initial and ongoing assessments of skills, knowledge, expertise, conduct and integrity. We achieve this through our recruitment, induction and appraisal procedures. See the firm's employee screening procedures for more information.

Independent audit function — Regulation 21(1)(c) MLR

The firm has established an independent audit function. The MLRO/MLCO completes monthly file AML audits to ensure that all employees are following the firms' policies and procedures and to identify any training requirements. The findings are referred to the firms' independent auditor, Nicola Robinson, to examine, evaluate, monitor, and make recommendations regarding the adequacy and effectiveness of its AML and CFT policies, controls, and procedures. The Independent Auditor reports findings & recommendations to the Directors.

Review of AML records

The MLRO/MLCO reviews the firm's AML records, including internal and external Suspicious Activity Reports and the findings of any independent audit, monthly to identify trends and risk areas requiring mitigation.

Economic Crime Levy ('ECL') — Part 3 Finance Act 2022

The ECL applies to entities regulated under the MLR with UK revenue exceeding £10.2 million per annum. The firm's annual turnover is below £10.2 million. ECL does not currently apply

AML training — Regulation 24 MLR

All relevant staff must complete AML training on induction and at least annually thereafter, tailored to their role and the risks identified in the FWRA. External agents, consultants and locums involved in regulated work must also receive appropriate training proportionate to their engagement.

The MLRO/MLCO is responsible for overseeing AML training across the firm. Training records are maintained by the MLCO and reviewed annually to ensure adequacy. Staff who have not completed allocated training will be followed up.

New starters

- all new starter fee earners and relevant support staff (including those who will deal with clients, handle client money or assist with compliance) are required to undertake and pass AML training, tailored to their position and business area, as part of their induction process, which includes the following key areas:
    - becoming familiar with the firm's AML PCPs
    - what the law on AML and terrorist financing is;
    - How the law applies within the context of the services provided by the firm;
    - how to undertake CDD checks in accordance with the firms' procedures;
    - when and how to carry out sanctions check;
    - recognising suspicious circumstances/ red flags to look out for;
    - how to report suspicions internally, non-reporting of suspicions is a criminal offence;
    - an understanding of what tipping off is and how to avoid doing it and record keeping and data protection requirements; and
    - record keeping and data protection requirements which are relevant to the MLR.

Ongoing training – internal

- all fee earners are required to undertake and pass online AML awareness/refresher training, which is reflective of the AML risks associated with their role and business area, at least annually, plus additional training, as required, to update on new developments.
- relevant support staff (including those who deal with clients, handle client money or assist with compliance) are required to undertake and pass online AML awareness/refresher training, which is reflective of the AML risks associated with their role, annually.
- relevant staff involved in the identification and verification process are familiar with the guidance provided by the UK Home Office on examining identity documents.
- a thorough debrief session will take place following the completion of annual AML training to ensure that the MLRO, MLCO and all relevant staff are on the same page in terms of understanding, key messages and objectives, performance measures to ensure learnings are applied and also to identify what additional training or support might be appropriate and a date for review.
- the MLRO and MLCO are required to undertake additional training or relevant AML-related qualifications to ensure they are competent to carry out their duties – for MLROs, this is to include training on the technical requirements of making disclosures to the NCA.
- The MLRO/MLCO will undertake regular file reviews from an AML perspective to ensure files are being handled correctly, in line with the firm's AML regime, and circulate details of the findings/areas for improvement/learning points to all relevant staff thereafter.
- the MLRO/MLCO will monitor publicly available information on best practice with regard to AML and CFT and will circulate summaries of relevant information, such as SRA thematic reviews, case law, regulatory decisions and legal press articles relating to real-life examples of where AML has come into play, as and when they come to light, by way of learning points and reminders to all relevant employees.
- Any material change to the legislative AML regime or the firm's internal policies will prompt a training review and refresher training for all relevant staff

You must undertake all allocated training, keep your training records up to date, and ensure you understand the requirements of this policy. See the firm's Learning and Development Policy for the overarching training strategy.

Risk assessments — Regulations 18 and 28(12) MLR

The firm's assessment of client and matter risk factors is set out in the firm-wide risk assessment. In response to those identified risks, the firm applies the following controls. High-risk clients or matters require enhanced due diligence ('EDD'). Simplified due diligence ('SDD') may be applied to certain low-risk cases. Standard due diligence applies to all other clients and matters.

Client and matter risk assessments

For **every** new client and matter, you must:

1. Complete the firm's client and matter risk assessment form (and update it as the matter progresses and in its final stages as part of ongoing monitoring).
2. Complete the firm's CDD form, concluding whether the overall money laundering risk is low, normal or high.

For each client and matter you must:

- Identify the client and the beneficiaries of the matter and understand the source of funds and wealth

- Understand the service you are providing, whether you have the expertise and risk appetite to deliver it, and how the service could be exploited for money laundering
- Understand why your services are needed and whether the rationale appears reasonable and genuine
- Be vigilant to red flags
- Determine what evidence you need to collect and what ongoing monitoring is required

You must continue to assess risk throughout the client relationship.

Client-level risk assessments

You must record a risk assessment for every client using the firm's approved form. The risk assessment must be signed off by the fee earner handling the matter and their supervisor before work begins. Higher-risk matters must be referred to the MLRO for approval.

Risk assessments are stored within the audit folder in the CMS.

The initial risk assessment must always be completed before the business relationship commences and in conjunction with CDD checks. Regulation 28(13) requires you to consider the purpose of the matter, the size of matters undertaken, and the duration of the business relationship (including significant gaps).

Matter-level risk assessments

A matter-level risk assessment should generally be undertaken for every new matter, kept updated, and signed off by the fee earner and their supervisor.

As part of your assessment, you should also consider whether:

- the client's financial circumstances, main business activities, source of wealth and source of funds align with the background and wider profile of the client;
- the structure, complexity or nature of the client entity or relationship makes it difficult to identify the true beneficial owner or any controlling interests;
- the client appears to be attempting to obscure understanding of their business, ownership or the nature of their matters;
- the client is a domestic/non-domestic PEP, or is closely related to or associated with a domestic/non-domestic PEP;
- the instruction from the client is channelled through a 3rd party and there is a lack of direct interaction with the client;
- there are any geographic risks associated with the client;
- the client wishes to conduct the business relationship or request services in unusual circumstances;
- the firm is aware that clients hold residence rights or citizenship in a jurisdiction in exchange for capital transfers, purchase of property or government bonds, or investment in corporate entities in that jurisdiction;
- negative/adverse media or press coverage is apparent regarding the client; and
- the client is seeking advice or implementation of an arrangement that has indicators of a tax evasive purpose, whether identified as the client's express purpose, in connection with a known tax evasion scheme or based on other indicators from the nature of the matter.

The following client- and matter-level risk factors should be considered as part of your matter risk assessment:

- the size, nature, purpose, commercial rationale, context or complexity of the matter are unusual or unclear;

- the source of wealth or funds involved in the matter is unclear or obscured;
- there is involvement of or payment to or from 3rd parties, especially where the relationship between the parties does not be appear clear or the payments do not make sense in the overall transaction;
- there is difficulty in identifying structures/beneficiaries/interests involved in a matter;
- the matter involves structuring of a transaction which obscures understanding of the nature of the transaction or ownership of the entities involved; and
- the level and type of matter do not fit the client's profile or involves a sector in which the client would not ordinarily operate.

Proliferation financing — Regulation 18A MLR

Regulation 18A of the MLR requires firms to assess and document their exposure to proliferation financing.

Proliferation financing is defined as the act of providing funds or financial services for use, in whole or in part, in the manufacture, acquisition, development, export, trans-shipment, brokering, transport, transfer, stockpiling of, or otherwise in connection with the possession or use of, chemical, biological, radiological or nuclear weapons, including the provision of funds or financial services in connection with the means of delivery of such weapons and other CBRN-related goods and technology, in contravention of a relevant financial sanctions obligation.

The National Risk Assessment on Proliferation Financing states that there might be:

- Direct proliferation financing (when there is a clear link between financing and proliferating factor) This might include evasion of sanction regimes.
- Indirect Proliferation Financing Activity (where there are more steps between financing and the proliferating actor).
- Proliferation Financing undertaken by state actors.

The firm's onboarding procedures — including CDD checks, risk assessments, and source of funds/wealth checks — enable us to identify and assess proliferation financing risks, including exposure to high-risk jurisdictions and clients or intermediaries potentially linked to proliferation financing or dual-use trade.

Staff must have a general awareness of proliferation financing risks. This is included in our AML refresher training.

If any red flag relating to potential proliferation financing is identified during onboarding or the course of a matter, you must speak with the MLRO immediately. The matter must not proceed without MLRO approval.

The MLRO will assess the risks and determine whether external reporting is required (including to OFSI, the NCA, or other enforcement agencies).

Customer due diligence ('CDD') — Regulations 27–30 MLR

The firm's assessment of the risks arising from its geographic exposure, delivery channels and transaction types is documented in the FWRA. The CDD requirements below are the firm's controls in response to those assessed risks. The MLR require you to carry out CDD when you do regulated work, before the business relationship commences. CDD involves:

- Identifying and verifying the client's identity

- Understanding the client's background and circumstances (including financial position) and assessing whether the legal services are consistent with that understanding
- Identifying the person instructing us on behalf of a client and checking they are authorised to act
- Taking reasonable measures to understand the ownership and control structure of any company, trust or other entity
- Identifying any beneficial owners and taking reasonable measures to verify their identity — where applicable, to equivalent standards as for individual clients
- Reporting material discrepancies to Companies House between information held and the PSC register (and other relevant registers, including the Register of Overseas Entities) where reasonably considered to be linked to money laundering, terrorist financing, or concealment
- Assessing the purpose and intended nature of the business relationship
- Conducting ongoing monitoring of the business relationship including, where necessary, the source of funds

You cannot forgo CDD based on long-standing or personal relationships. However, these factors may inform your risk-based approach.

Cash policy

The firm does not accept money in cash, save for fees and disbursements up to a limit of £500 in any 28-day period. If anyone asks you to accept more than this in cash, report the request to the MLRO.

When to complete the CDD form

You must complete the firm's CDD form:

- When taking on a new client
- When opening a new matter for an existing client

You must also run fresh checks if:

- The client's risk profile has changed significantly
- There is any indication that a beneficial owner has changed
- You suspect money laundering or doubt the veracity of documents previously supplied

The completed form and evidence of identity must be filed in the audit folder in the CMS.

On purchase matters you will be required to complete Source of Funds and Source of Wealth documentation to confirm that this has been considered. If the Thirdfort report identifies that the client is a PEP, and investigations confirm this is the case then a PEP Risk Assessment Form should be completed and submitted to the MLRO before any services are provided. If the Thirdfort report flags that the client is possible a PEP, but investigations prove this not to be the case (i.e. in cases of a similar name, then this should be detailed on the client due diligence form).

Client identification and verification

Identification means being told the client's name, address and date of birth. Verification means obtaining evidence from an independent and reliable source to support that identity. We cannot rely solely on the Companies House register for verification.

Timing:

Verify the client's identity (and any beneficial owner) **before** commencing the business relationship and before any money is taken. Be alert to deepfake fraud risks. Identity verification must be completed as soon as practicable. Do not accept money on account (other than modest

disbursements) or carry out substantive work until verification is complete. You must also have regard to the source of funds & wealth requirements on page fourteen.

Documents:

Satisfy yourself that documents are originals. Ensure any photographs provide a likeness. Take copies, sign and date them. You should obtain either one government document verifying name, address and date of birth, or a government document verifying the full name supported by documents verifying address and date of birth. Proof of address should follow GOV.UK guidance where possible. Where government-issued documents are unavailable, consult the LSAG guidance (section 6.14.7) and speak with the MLRO.

Clients not physically present:

Not meeting a client in person does not prevent verification but adopt a risk-based approach. Additional steps may include using digital ID&V services meeting MLR requirements and address verification codes. Where certified copies are relied upon, document the risks in the matter-level risk assessment.

Intermediaries, agents and representatives:

You must identify and verify the intermediary's identity and authority. Where a law firm or professional intermediary instructs you for the benefit of their client, you must undertake CDD on the firm (SDD may be appropriate), and the underlying client is a beneficial owner for CDD purposes.

Renewing CDD

Operate a system of regular review and renewal:

- Review CDD upon each new matter, particularly after a significant gap between instructions
- Update CDD when you become aware of changes to identification information

You must also carry out CDD on existing clients if you suspect money laundering or doubt previously supplied documents.

Overseas entities acquiring UK property — Economic Crime (Transparency and Enforcement) Act 2022

Under the Economic Crime (Transparency and Enforcement) Act 2022, with effect from 01.08.22, Companies House maintains a register of overseas entities who own UK property.

An overseas entity is defined as a legal entity governed by the law of a country or territory outside the UK (which includes Crown Dependencies and British Overseas Territories).

An overseas entity wishing to buy, sell or transfer property or land in the UK (which includes all freehold estates and leasehold granted for a term of more than 7 years) must provide details to Companies House of its beneficial owners or the managing officers who control it.

Upon registration, the entity is issued with an overseas entity ID – without this, no dispositions will be entertained by HM Land Registry.

Each overseas entity will be required to update its ownership entry details at Companies House on an annual basis.

It is the firm's policy that we would not act for overseas entities in buying, selling or transferring of land in the UK.

Levels of CDD — Regulations 28, 33 and 37 MLR

Standard due diligence — Regulation 28 MLR

The default level of check you should apply to all low risk and medium risk clients and matters, unless there is reason to apply SDD or EDD (see below)

- involves identifying the client and verifying their details using reliable, independent source documents, data or information – this includes identifying and verifying the details of anyone acting on behalf of the client.

- Also requires gathering information to enable you to understand the nature of the business relationship.

- In addition, there is a requirement to conduct ongoing due diligence on the business relationship and scrutinise transactions undertaken throughout the course of that relationship to ensure that they are consistent with your knowledge of the client, their business and risk profile, including, where necessary, the source of funds.

- Our firm's standard due diligence is carried out by way of a full Thirdfort online verification or with passport/driving licence alongside a Thirdfort Lite verification. Any other must be approved by the MLRO.

Simplified due diligence ('SDD') — Regulation 37 MLR

Whilst the MLR permit simplified due diligence measures to be applied where there is a low risk of money laundering, we take the view that at least our standard identification procedures should be applied in all cases except where the MLRO agrees otherwise.

However, SDD may be appropriate when instructed by:

- a credit or financial institution which is subject to requirements in national legislation/are regulated by the FCA;
- a public administrator or a publicly owned enterprise;
- regulated professional firms, such as accountants and solicitors;
- an individual resident in a geographic area of lower risk/who does business in a geographic area of lower risk;
- reputable charities registered with the Charity Commission;
- a company listed on a regulated market (including majority owned subsidiaries).

In such low-risk cases you may be able to accept assurances (in writing) from the person instructing you as to the identity of beneficial owners, rather than insisting on seeing their identifying documents.

SDD **is not appropriate**, and you must cease applying it and apply a higher standard of due diligence if:

- you doubt the truth of any documents submitted for identification or verification;
- a risk assessment you do identifies that it is not an instance of low risk;
- you suspect money laundering or terrorist financing;
- the risk profile changes for the worse - it is important to continue to monitor the business relationship and transaction to enable you to detect any unusual or suspicious transactions throughout the life span of the matter;
- there is an obligation to apply EDD under MLR 33(1).

Where you have assessed that it is appropriate to apply SDD in the circumstances, this must be approved first by the MLRO).

Enhanced due diligence ('EDD') — Regulations 33–35 MLR

You must carry out EDD where the client or transaction presents a higher risk. Maintain a specific list of EDD matters for SRA reporting purposes. EDD is always required where:

- Any party is established in a High-Risk Third Country ('HRTC')

The amended MLR's which are due to come into effect on the 30th of June 2026, state only FATF Call for Action countries will trigger mandatory EDD (currently Democratic People's Republic of Korea, Iran & Myanmar). However, the firm has decided that we will continue to include the FATF Increased Monitoring countries as High Risk and we will also continue to carry out EDD on those matters.

The FATF Increased Monitoring list was last updated on the 19th of June 2026, and they identified the following countries as subject to increased monitoring:

Angola, Bolivia, Bosnia and Herzegovina, Bulgaria, Cameroon, Côte d'Ivoire, Democratic Republic of Congo, Haiti, Iraq, Kenya, Kuwait, Lao Peoples Democratic Republic (Laos), Lebanon, Monaco, Nepal, Papua New Guinea, South Sudan, Syria, Venezuela, Vietnam, Virgin Islands (UK) and Yemen.

Check current status at client onboarding:

- The client is a PEP, family member or known close associate of a PEP (greater EDD for non-domestic PEPs)
- The client has provided false or stolen identification
- The corporate structure is unusual or excessively complex
- A transaction is unusually complex or unusually large with no apparent economic or legal purpose, or involves unusual patterns
- Any other case presenting a higher risk

Where any party is established in an HRTC, EDD must include: obtaining additional independent evidence, better understanding the background and financial situation (including source of funds and wealth), ensuring the transaction is consistent with the client's financial profile, obtaining information on the reasons for the transaction, obtaining senior management approval, and conducting enhanced monitoring.

In addition, you should be aware of the following risk factors which particularly apply in the context of this firm. Property work carries a particularly high risk of money laundering.

Factors which may make property work particularly high risk include:

- high value purchases, particularly if they do not involve a mortgage;

- funds being provided by someone other than the client or a mortgage lender;
- clients who are otherwise unable to provide convincing explanations of their source of funds or source of wealth;
- rapid purchase and sale of property;
- transactions involving multiple law firms;
- clients that are non-domestic PEPs from high corruption – risk jurisdictions and those charged with/alleged to have committed corruption offences.

In such cases you should discuss what extra precautions are required with the MLRO (*or the MLCO*). Precautions may include fuller evidence of identification (for example of beneficial owners), taking up references, and monitoring rigorously the source of funds both initially and throughout the matter.

Where any party to a transaction on which we are instructed is established in a high risk third country (as defined by the UK) the MLR specifically require that EDD measures must include:

- obtaining additional independent, reliable evidence to verify the information provided by the client and the client's beneficial owner;
- taking additional measures to better understand the background, ownership and financial situation of the client and if appropriate the other parties involved – which will include source of funds and source of wealth evidence for the client and the client's beneficial owner;
- taking further steps to ensure that the transaction is consistent with your understanding of the client's financial profile;
- obtaining additional information on the incidental nature of the business relationship;
- obtaining information on the reasons for the transaction;
- obtaining the approval of senior management for establishing or continuing the business relationship;
- conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination.

Where work must start before CDD is complete, you must first obtain MLRO approval.

Ongoing monitoring — Regulation 28(11) MLR

You must conduct ongoing monitoring of business relationships. Ongoing monitoring is defined as:

- scrutiny of transactions undertaken throughout the course of the relationship, (including where necessary, the source of funds), to ensure that the transactions are consistent with your knowledge of the client, their business and their risk profile; and
- undertaking reviews of existing records and keeping the documents, or information obtained for the purpose of applying CDD, up to date.

Ongoing monitoring should normally be conducted by the fee earners handling the retainer and involves staying alert to suspicious circumstances which may suggest money laundering, terrorist financing, or the provision of false CDD material. The higher the risk the client and the transaction pose, the more rigorous should be your ongoing monitoring.

All matters are appropriately supervised. In addition, high risk matters are directly supervised by Directors & MLRO.

As outlined above, you should operate a system of regular review and renewal of CDD and take a risk-based approach to such activity. You should consider reviewing (although not necessarily redoing) the CDD upon each new matter. Where there has been a significant gap between instructions (anything above a year may be considered a significant gap in relation to those clients or transactions assessed as higher risk), you should consider refreshing the CDD.

CDD must also be updated when you become aware of changes to the client's identification information (e.g. changes of name, address, beneficial owner, etc.). And according to Regulation 27(9), you must apply (or re-apply) CDD measure to an existing client on a risk-based approach when circumstances of that client relevant their risk assessment have changed. In determining this, you must consider:

- any indication that the identity of the client or beneficial owner has changed;
- any transactions which are not reasonably consistent with your knowledge of the client;
- any change in the purpose or nature of the relationship; and
- any other matter which may affect your assessment of the money laundering or terrorist financing risk in relation to the client.

As noted in the CDD section above, it is a requirement to report to Companies House on any material discrepancies noted between information held and the PSC register and other relevant registers including the Register of Overseas Entities. This applies while undertaking CDD checks and carrying out ongoing monitoring.

You must also be aware of obligations to keep clients' personal data updated under the Data Protection Act 2018 and the UK GDPR or their equivalent.

Source of funds and source of wealth

Before accepting any funds into the Client Account, both checks must be completed, except where the funds are for modest disbursements, such as search fees, or a modest payment on account of anticipated costs. This requirement applies regardless of how well you know the client or how long the relationship has existed.

According to the Legal Sector Affinity Group AML Guidance, 'understanding the *source of funds* and *source of wealth* is a key protection for your practice, and it should be approached as an opportunity to protect your practice from being used for money laundering.' Both checks must be completed before any funds are accepted into the Client Account.

Please note that source of funds and wealth checks may be required not only when dealing with transactional work. This is also applicable for the tax advice, company's services, etc. If unsure, please speak with the MLRO for further guidance.

Source of funds refers to the origin of the funds used to fund the specific transactions or activities that occur within the client's business relationship with you. Checking this means looking into:

1) where those funds came from;
2) how they were accrued by the client (or any third party who has provided the client with funds);

3) ensuring a risk-based approach that they are not the proceeds of crime.

The information obtained should be substantive and establish a provenance or reason for having been acquired e.g. salary, gift etc.

Checking source of funds often requires some understanding of the client's (and third parties who have provided funds) source of wealth.

Source of wealth refers to the origin of the client's total assets and checking this involves asking why and how the client/third party who has contributed funds has the amount of overall assets they do and how did they accumulate/generate these?

Evidence must be obtained to support information provided by the client – it is never sufficient to rely on anecdotes or perceptions of how a client acquired their wealth.

The amount of verification necessary will depend on the amount of risk presented by the client and matter. Enhanced checks will need to be carried out in high-risk circumstances; in which case you should consult the MLRO to decide on approach to be taken.

It is very important to document the source of funds and source of wealth checks carried out clearly on the file as evidence of the enquiries made and the thought process behind decisions. A summary of the checks must be clearly identifiable, should a third party such as an auditor or regulator, review the file.

Best practice is to carry out source of funds and source of wealth checks at the earliest opportunity, when completing CDD checks, as any issues are likely to be far more disruptive if they come to light in the later stages of a transaction e.g. exchange or completion in a property transaction.

Source of funds – property purchase, etc
When acting for someone who is purchasing property or entering into any other large financial transaction you should understand how they will be funding the transaction. This is both to meet our "ongoing monitoring" obligation and to check that their funding arrangements comply with their mortgage offer.

In circumstances where it becomes known that a third party is to contribute to funds for a transaction, you should consider also seeking to understand and obtain evidence relating to the third party's underlying source of funds, in the same way you would on the client themselves, with the extent of such measures increasing with risk level. Whether and the extent to which you should obtain, review and evidence third party source of funds is dependent upon the risk profile of the client or matter, bearing in mind that accepting payments from unknown or unassociated third parties is a specific risk factor pursuant to 33(6)(b)(iv).

Ask the client to complete a Source of Funds and Source of Wealth Questionnaire. Alternatively, you can complete and sign the form yourself, based on discussions with the client.

When applying standard CDD, you should request some form of evidence of source of funds, such as bank statement, Wills, full payslips, audited financial accounts and sales/purchase agreements. You need to be satisfied that you understand where the money is coming from and why and that the transaction makes sense.

Adopt a risk-based approach to weigh up the information provided and whether it is consistent with what you know about the client. If the client gives inconsistent or implausible information, you should seek further evidence and discuss the matter with the MLRO/MLCO.

Beneficial ownership — Regulations 28 and 42–44 MLR

When instructed on behalf of any company, partnership, trust or other principal, you must take reasonable measures to:

- Check the identity of the person instructing you and confirm their authority
- Understand the client entity's ownership and control structure (not just percentages, but identifying individuals with control and directing power)
- Determine and verify the law to which the body corporate is subject, its constitution, board of directors (or equivalent), and senior persons responsible for operations
- Identify any beneficial owner and take reasonable measures, on a risk-sensitive basis, to verify their identity
- Check that beneficial owners are properly recorded in applicable registers (PSC Register, Trusts Registration Service) — report material discrepancies to Companies House immediately unless protected by legal professional privilege. Note: the PSC register alone is not sufficient for identifying beneficial owners.

A beneficial owner is broadly: for a body corporate or partnership, an individual with ultimate control or who owns/controls (directly or indirectly) more than 25% of shares or voting rights; for a trust, each of the settlor, trustees and beneficiaries.

Trust and company services — terrorist financing risk: Although legal services overall are assessed as presenting a low terrorist financing risk, the National Risk Assessment has raised the terrorist financing risk rating for trust and company services specifically from low to medium. Staff providing these services should apply a correspondingly higher level of vigilance to control and beneficial ownership arrangements, in addition to the money laundering risk considerations set out above.

Where a company instructs the firm and the directors giving those instructions are not its sole beneficial owners, the matter must be referred to the MLRO before we continue acting. If the MLRO gives authority to proceed, the reasons for that decision must be clearly documented.

Checking beneficial owners

The goal is to understand who the natural persons are who own and control the client, and in whose interests, it is operating. It will rarely be necessary to consult the detailed definition of a beneficial owner if you keep that principle in mind.

More guidance about who is a beneficial owner and the evidence required is in the notes which accompany the CDD Form. If in doubt, consult the MLRO/MLCO. However, bear in mind these principles:

- you do not always have to see evidence to verify the identity of all beneficial owners. It depends on the risk level;
- if we are instructed by a business, in most cases you should obtain the same evidence to verify the identity of the beneficial owner(s) you would if they had instructed you directly as the client. However, in the case of large, well-established businesses with many people involved you may not need to see the documents of all beneficial owners;

- if it seems the client may be a mere nominee or front for another person, insist on full and strict verification of that other person's identity, as well as that of the client. Also discuss the matter with the MLRO/MLCO.

If you are unable to identify or verify the Ultimate Beneficial Owners, *you should review the identity and verification of people with significant control/ refer the matter to the MLRO.*

Reliance — Regulation 39 MLR

The firm does not rely on third parties to carry out CDD on its behalf. All CDD must be carried out by the firm directly. If other organisations ask to rely on our CDD, refer the request to the MLRO/MLCO.

Record keeping — Regulation 40 MLR

We are required under Regulation 40 MLR to maintain AML records (including client identification and transaction records) for a minimum of five years from completion of the transaction or end of the business relationship. CDD records relating to transactions within a business relationship need not be retained for more than ten years.

Taking the above into account, our internal procedure is to retain the complete file of papers, including CDD records, for six years.

Personal data is protected by data protection legislation and must be used only for the purposes of preventing money laundering unless otherwise authorised.

Transferring clients between departments

When a client transfers between departments, a fresh AML assessment must be carried out. This is particularly important for transfers from lower-risk departments (e.g. litigation, employment) to higher-risk departments (e.g. property, corporate). The receiving department must ensure: a fresh risk assessment, review of CDD including beneficial owners, PEP status and source of funds, and fresh conflicts checks where new parties are involved.

Transferring clients between jurisdictions ('passporting')

We have assessed the risk of "passporting" (where a client instructs a firm on a low-risk matter to avoid scrutiny on a later high-risk matter). To mitigate this risk, we assess and complete CDD on all matters.

Politically exposed persons ('PEPs') — Regulation 35 MLR

You must obtain approval from the MLRO and/or responsible person or authority before accepting a PEP as a client.

A PEP Risk Assessment must be completed and submitted to the MLRO as soon as you are aware that we are dealing with a PEP. As the Solicitors Regulation Authority asks firms for data on how many clients have been identified as PEPs, we keep a central record.

Who is a PEP?

A PEP is a person who is entrusted with prominent public functions, whether in the UK (domestic PEP) _or abroad (non-domestic PEP), other than as a middle-ranking or more junior official. Examples include:

- heads of state, heads of government, ministers and deputy or assistant ministers;
- members of parliament or similar legislative bodies;
- members of governing bodies of political parties;
- members of the supreme court;
- members of courts of auditors or of the boards of central banks;
- ambassadors, diplomats and high-ranking officers in the armed forces;
- members of the administrative, management or supervisory bodies of State-owned enterprises;
  directors, deputy directors and members of the board or equivalent function of an international organisation.

The MLR refer to the starting point for the customer due diligence assessment as a lower risk for a domestic PEP than a non-domestic PEP, therefore it is important to ascertain which applies.

A person must also be treated in the same way as a PEP if that person is a family member or known close associate of a PEP

If a person has been a PEP but no longer holds the relevant public function, that person must nevertheless be treated as a PEP for at least 12 months after ceasing to hold the public function. A period of more than 12 months may be appropriate for some former PEPs due to the positions they held and the corresponding risk.

PEPs and CDD

- Our procedure for determining whether a client is a PEP or a family member or known close associate of a PEP is primarily using our online verification platform (Thirdfort). Once identified, a PEP Risk Assessment must be completed and submitted to the MLRO so the correct level of risk can be applied.

- If you act for such a person, you will also be required to take extra measures to establish the source of wealth and the source of funds involved.

- You must also conduct closer enhanced ongoing monitoring of the business relationship for the lifespan of the matter. The extent of the extra measures and ongoing monitoring should be discussed with the MLRO.

5. Procedures

Reporting suspicious circumstances — ss.330–332 POCA, s.21A Terrorism Act 2000

You must report anything giving grounds to suspect money laundering or terrorist financing to the MLRO, without delay. **Failure to report is a serious criminal offence.**

If there is something unusual, it is normally appropriate to make enquiries of your client or a third party to clarify and help decide whether you have a suspicion. Such enquiries do not amount to tipping off.

How to report:

1. Speak to the MLRO informally about your concerns. The MLRO will consider all circumstances (including privilege) and advise you.

2. If the MLRO advises a formal disclosure, they will provide you with a report form.
3. The MLRO will decide whether to report externally to the NCA within the NCA reporting timescale, seek consent to proceed with any transaction (DAML), and whether to notify other enforcement agencies (e.g. HMRC, the police).

Privilege

Legal professional privilege may apply. Three types are recognised: common law legal advice privilege, common law litigation privilege, and the statutory privileged circumstances in section 330(6) POCA.

You should not report where the information was communicated in privileged circumstances — by the client or their representative in connection with legal advice, or by any person in connection with actual or contemplated legal proceedings.

Important:

A client cannot claim privilege where they intend to use the firm's services to launder money (the crime/fraud exception). Even where privilege prevents a report, it is still an offence to be involved in a money laundering transaction (ss.327–329 POCA) — you may still need to cease acting.

Two additional defences are available under the Economic Crime and Corporate Transparency Act 2023. First, the de minimis exemption: a DAML SAR is not required where the criminal property is valued at less than £1,000 and the transaction takes place in the regulated sector. Second, the mixed-property transactions exemption may apply in certain circumstances where the proceeds of crime form part of a mixed-property transaction. If either may apply, consult the MLRO before proceeding.

If privilege may apply, have an off-the-record conversation with the MLRO before determining how to proceed. Where you do not report due to privilege, clearly document your decision-making process on the file.

Tipping off — ss.333A–333D POCA

If you suspect money laundering or terrorist financing, report **only** to the MLRO. You must not tip off the suspected person — including informing them that a report has been made or an investigation is being carried out or contemplated.

The MLRO will guide you on what information you may give and to whom, including how to explain to a client that you are declining to act further if appropriate.

Exceptions to tipping off offences:

- **Disclosures within the firm (s.333B POCA):** permitted, but we recommend speaking only to the MLRO to maintain confidentiality
- **Disclosures to other law firms for the purpose of preventing money laundering (s.333C POCA):** where relating to a shared client or transaction. Seek MLRO approval before disclosing
- **Disclosures to a client to dissuade them from money laundering (s.333D POCA):** with MLRO approval, you may inform the client that continuing may constitute a criminal offence and that the retainer may be terminated

Sanctions

You must carry out sanctions checks in every matter and on a regular basis thereafter where the firm has identified that a client could become subject to future sanctions.

Where you suspect that someone involved in a matter is subject to sanctions or has committed an offence under sanctions regulations, you must inform the MLRO without delay and take no further action unless the MLRO tells you otherwise. The MLRO will investigate and, where appropriate, report to the Office of Financial Sanctions Implementation ('OFSI').

See the firm's **Sanctions Policy** for detailed requirements on sanctions screening and compliance.

Technology

To comply with our AML duties, we use the Thirdfort Identification Verification Platform.

If we change our products, technology or business practices, we will assess and mitigate associated risks.

Responding to AML enquiries from authorities

All enquiries from the police, the NCA, the SRA or other bodies about AML issues must be referred immediately to the MLRO, who will investigate and respond as appropriate.

6. Regulatory Framework and References

SRA Principles

- Principle 1: Upholding the constitutional principle of the rule of law, and the proper administration of justice
- Principle 2: Upholding public trust and confidence in the solicitors' profession and in legal services provided by authorised persons
- Principle 4: Acting with honesty
- Principle 5: Acting with integrity
- Principle 7: Acting in the best interests of each client

SRA Code of Conduct for Firms

- Paragraph 2.1: Effective governance structures, arrangements, systems and controls to ensure compliance with all regulatory obligations, including identifying, monitoring and managing risks
- Paragraph 2.2: Keeping and maintaining records to demonstrate compliance with obligations under the SRA's regulatory arrangements
- Paragraph 9.1&9.2: Compliance officers (COLP and COFA) who are suitable and competent

Legislation

- Proceeds of Crime Act 2002 ('POCA') — as amended, in particular ss.327–332 and ss.333A–333D
- Terrorism Act 2000, in particular s.21A
- Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ('MLR') — as amended by SI 2019/1511, SI 2022/860, SI 2022/1336 and SI 2023/1371 **and SI 2026/621**
- Economic Crime (Transparency and Enforcement) Act 2022

- Economic Crime and Corporate Transparency Act 2023
- **Crime and Policing Act 2026, section 250 (corporate criminal liability where an offence is committed by a senior manager)**
- Finance Act 2022, Part 3 (Economic Crime Levy)

Guidance

- LSAG AML Guidance for the Legal Sector (approved by HM Treasury, effective 23 April 2025)
- SRA AML guidance: https://www.sra.org.uk/solicitors/guidance/topic/money-laundering/
- **SRA Sectoral Risk Assessment — Anti-money laundering, terrorist financing, proliferation financing and sanctions (latest edition): https://www.sra.org.uk/sra/research-publications/aml-risk-assessment/**
- SRA Thematic Review on AML Training
- National Risk Assessment on Proliferation Financing
- HM Treasury National Risk Assessment of Money Laundering and Terrorist Financing (latest edition)

Accreditation

- Lexcel v6.1 — section 5.13 (AML policy requirements)
- CQS CPMS — section 5.12(j) (inter-departmental transfer requirements)

Review of policy
This policy will be reviewed at least annually by Timothy Halliday (MLRO)