**Anti-Money Laundering Policies and Procedures**

**Firm name:**

**Date:**

Version control:

|  |  |  |
| --- | --- | --- |
| Date | Change | Name |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. **Overview 1**
2. **Obligations 2**
3. **Risk Assessment and Verification 2**
4. **Responsibilities and Training 4**
5. **Quality Assurance and Record Keeping 5**
6. **Further Information 5**
7. **Overview**

**(Firm Name)** take a zero-tolerance approach to being involved in illegal/illicit activity and will fully comply with all relevant sections of the Money Laundering Regulations (ML Regs), the Proceeds of Crime Act 2002 (POCA), and the Terrorism Act 2000 (TACT).

All partners and employees of the firm are under an obligation and duty to comply with the above. This policy and any related procedures aim to help partners and staff fulfil these responsibilities, by providing a clear framework, along with setting out the firm’s key principles and obligations.

* Failure to fulfil these responsibilities may result in disciplinary action and may also result in criminal sanctions for the staff involved.
* Breaches may also be reportable to our AML Supervisor (The Law Society of Scotland) which may result in professional disciplinary action.
* Furthermore, a report may also have to be made to the NCA or other law enforcement agencies, which may result in a criminal investigation.
1. **Obligations**

Responsibilities under the Money Laundering Regulations 2017 (MLRs 2017) and the Proceeds of Crime Act 2002 (POCA 2002) include:

* Risk-based assessment
* Customer Due Diligence, including Identification and Verification (ID&V) requirements, assessing Source of Wealth (SoW), and application of Know your Client (KYC) information
	+ Enhanced Due Diligence and ongoing monitoring (incl. definition and treatment of PEPs)
* MLRO Responsibilities, Suspicious Activity Reporting, Tipping Off, Police Orders
* Quality Assurance
* AML Record Keeping
* AML Training
* Compliance with International Sanctions Requirements

Key responsibilities of staff therefore include (but are not limited to):

* Conducting an adequate risk assessment and appropriate due diligence (CDD) on clients and transactions, including PEP and sanctions checking.
* Monitoring all clients/transactions on an ongoing basis for potential money laundering or terrorist financing activity;
* Reporting any suspicious activity in respect of client or transactions, to the MLRO in accordance with the firm’s SAR (suspicious activity reporting) procedure
* Avoiding discussing any potential or actual SARs with clients or any third parties (“Tipping off”)
* Referring any Police/Law Enforcement queries or requests to the MLRO
* Undertaking any AML-related training provided by the Firm.
* Keeping appropriate records of all AML related activity
1. **Risk Assessment and Verification**

**Firm risk profile**

This may be a summary of a separate r.18 firm level risk assessment or (if appropriate to the size and nature of your practice) the firm level risk assessment itself may be noted in full below

The partners believe **(Firm Name)** is at an inherently high/medium/low risk of being used to launder the proceeds of crime. This is based on the following factors:

* Types of work undertaken – regulated/non-regulated. Mostly Property? Litigation? Wills/Executry? Etc.
* High turnover of clients or a stable existing client base?
* High proportion of one-off clients/deals?
* Mostly face-to-face or face-to-face contact with clients?
* Geographical location of practice – high levels of crime?
* Act for clients across both criminal and civil matters
* International element to your business

AML policies, procedures and controls should be tailored to mitigate the risk as noted above. I.e. if your firm level risk assessment indicates conveyancing as a higher risk area of your business, it may be appropriate to place stronger/more stringent AML procedures in place in this area of your business, compared to lower risk areas.

**Risk assessment**

Detail your firm’s approach to risk assessment, including

* Who is responsible for risk assessment/how it is undertaken?

(Link into Risk Assessment Form used by firm)

* Client
* Transactional
* When/How Often reviewed
* High level overview of risk factors/ ‘red flag indicators’
* Firm position/policy re International clients/transactions – especially from non-EU countries
* Should control what happens when red flags/risks are identified and what standard of due diligence should then be applied, and what this entails
* Examples/type of evidence which should be held

**Customer due diligence**

Detail your firm’s procedures for taking ID&V, KYC, SoW checks, ongoing monitoring etc. See the AML section on the Law Society‘s website for further information/support)

* Who is responsible for taking ID&V and how this is undertaken?
* Timing of ID&V
* ID&V requirements for private individuals, companies, trusts and other legal entities – who/what should be ID’d etc.
* Acceptable ID Documents
* Simplified – in what situations – listed/regulated companies etc.
* Standard – what is the standard ID&V undertaken
* Enhanced – in what circumstances and what is undertaken over and above standard (primarily evidence of SoW, ongoing monitoring etc.)
* Using reliance as per r.39 of the MLRs 2017
* Electronic Verification
* 3rd party funding ID&V requirements (immediate family/unrelated)
* Any value limits to cash transactions handled/accepted by the firm

**Politically exposed persons (PEPs)**

The firm will apply enhanced and ongoing due diligence to all PEP clients and will consider and assess the heightened risk of undertaking business with or on behalf of PEPs, particularly the risk of laundering the proceeds of corruption.

If the you deploy an electronic verification tool – this tool should be used to check potential PEP status on all clients

If electronic verification is not deployed and circumstances or information arise to suggest that a client is a PEP (or a corporate client is owned/controlled by a PEP) you should ask the client additional questions to determine PEP status, and use open source information to verify

What is a PEP?

* A ‘politically exposed person’ (PEP) is a term describing someone who has been entrusted with a prominent public function.
* A PEP generally presents a higher risk for potential involvement in bribery and corruption by virtue of their position and the influence that they may hold. Positions may include:
	+ Head of state, heads of government, ministers and deputy or assistant ministers
	+ Members of parliament
	+ Members of supreme courts, of constitutional courts, or of other high-level judicial bodies – members of courts of auditors or of the boards of central banks
	+ Ambassadors, charges d'affairs and high-ranking officers in the armed forces
	+ Members of the administrative, management or supervisory bodies of state-owned enterprises

The definition of a PEP also extends to:

* family members of a PEP – spouse, partner, children and their spouses or partners, and parents
* known close associates of a PEP – persons with whom joint beneficial ownership of a legal entity or legal arrangement is held, with whom there are close business relationships, or who is a sole beneficial owner of a legal entity or arrangement set up by the primary PEP

**International sanctions checking**

The firm will conduct a sanctions list check on each new client via the HM Treasury website (or an electronic verification system if used) to check if the client or source of funds is related to a sanctioned jurisdiction/regime, and conduct ongoing checks periodically (at least annually for all clients) <https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets>

1. **Responsibilities and Training**

**MLRO responsibilities/ Suspicious Activity Reporting (SARs)**

The MLRO of the firm is…… He/she is responsible for:

* Scrutinising of unusual transactions highlighted to him/her
* Ultimately deciding when/ if a client to be taken on where there is a high risk of money laundering
* Reviewing SARs made from employees - decide when to submit to NCA
* Dealing with any contact to or from the Law Society or Police
* Ensuring all staff trained to level appropriate to their role

Further detail in this section should include:

* Detail how staff should make reports to the MLRO
* Make it clear obligations under POCA are mandatory – criminal offences
* Detail tipping off definition and potential issues
* What should be included in reports
* Timing of reports
* What process should be followed in the event of a Police Order being served

**AML training of partners and staff**

Procedures should detail:

* Which staff require what training (specific to role)
* What form the training will take
* How often training should take place
* How staff will be kept up to date with emerging risk factors/new developments for the firm
1. **Quality Assurance and Record Keeping**

**Quality Assurance**

Detail how, and to what frequency the firm undertakes quality checking of compliance/AML files

**AML Record Keeping Section**

Detail how the firm manages, records and stores AML related material, incl. retention period Relevant records could be:

* AML policies, procedures, manuals
* Risk assessments
* CDD/KYC/SoW evidence
* Evidence of staff training
* Suspicious Activity Reports
* E-verification records
* PEP/Sanction screening searches

Firms need to keep adequate records of AML/CDD material – a list of relevant records is on the slide and should be kept for a minimum of five years after the relationship has ended or the transaction has been concluded.

**Related documents**

Detail any internal firm documents, checklists, procedures which underpin/support this policy.

Could be:

* Risk Assessment Form
* Internal SAR reporting form
* Acceptable ID List
1. **Further Information**

Law Society’s website , search [AML](https://www.lawscot.org.uk/members/business-support/financial-compliance/anti-money-laundering/)

Money laundering Regulations 2017:<http://www.legislation.gov.uk/uksi/2017/692/contents/made>

POCA 2002: <http://www.legislation.gov.uk/ukpga/2002/29/contents>