**Instructions**

* The Law Society has developed these sample adaptable Policies, Controls & Procedures (PCPs) to assist solicitors in complying with the obligation to have PCPs in place.
* This sample PCPs can be adapted by firms to suit their firm’s individual needs. No two PCPs will be the same.
* **Colour key:**
* Text in black can be used in your firm’s PCP.
* **Text in red outlines the statutory requirement to have a policy, control or procedure in place.**
* **Text in blue can be adapted and developed by firms to suit their specific compliance needs.**

**FIRM NAME: DATE:**

**VERSION CONTROL:**

|  |  |  |
| --- | --- | --- |
| Date | Change | Name of person reviewed by |
|  |  |  |
|  |  |  |

**POLICY STATEMENT/OVERVIEW SECTION**

**(Firm Name)** take a zero tolerance approach to being involved in illegal/illicit activity, and will fully comply with all relevant sections of the Criminal Justice (Money Laundering and Terrorist Offences) Act 2010 (‘the 2010 Act’), the Criminal Justice (Money Laundering and Terrorist Offences) (Amendment) Act 2018 and the Solicitors (Money Laundering and Terrorist Financing Regulations) 2016 (SI 533 of 2016).

It is important that all staff are aware of the serious consequences for failure to comply with statutory AML duties when the firm provides an AML-regulated legal service. It is a crime not to comply with statutory AML duties. It is equally important for all staff to ensure that they do not unwittingly commit the offence of money laundering by not being alert to money laundering red flags.

All partners and employees of the firm are under an obligation and duty to comply with the Act.

Section 54(1) requires firms to adopt internal policies, controls and procedures (PCPs) to prevent and detect ML and TF. These policies and any related controls and procedures aim to help partners and staff fulfil their responsibilities, by providing a clear framework, along with setting out, the firm’s key principles and obligations. Section 54(2) requires staff in solicitors’ firms to follow the firm’s PCPs when providing AML-regulated legal services.

**AML LEGISLATIVE FRAMEWORK SECTION**

Statutory compliance duties under the Act include:

* Business Risk Assessments
* Policies, Controls and Procedures (PCPs)
* Customer Risk Assessments to determine extent of Customer Due Diligence (‘CDD’) measures
* CDD measures
* Reporting
* AML Record Keeping
* AML Training

**AML-regulated legal services**

The above AML obligations only arise where a solicitor participates in certain types of legal work. This work is specified in the definition of the term “relevant independent legal professional” contained in section 24(1) as a solicitor who carries out any of the following services:

“(a) the provision of assistance in the planning or execution of transactions for clients concerning any of the following:

(i) buying or selling land or business entities;

(ii) managing the money, securities or other assets of clients;

(iii) opening or managing bank, savings or securities accounts;

(iv) organising contributions necessary for the creation, operation or management of companies;

(v) creating, operating or managing trusts, companies or similar structures or arrangements;

(b) acting for or on behalf of clients in financial transactions or transactions relating to land;”

Accordingly, legal activities falling outside these categories are exempt from AML CDD.

Irrespective of whether an AML-regulated legal service is being provided, a solicitor must always remain alert to the risk of unwittingly committing the substantive offence of money laundering or terrorist financing. See further Chapters 2 and 9 of 2010 Guidance and Section 2 of the 2018 Guidance.

**Verifying the identity of all clients irrespective of whether an AML-regulated legal service is provided**

It is the firm’s policy to follow the Law Society’s best practice guidance to verify the identity of **all** clients irrespective of whether statutory AML CDD arises.

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

* Conducting an adequate Customer Risk Assessment and appropriate CDD on clients and transactions;
* Staying alert to potential money laundering or terrorist financing activity;
* Reporting any suspicious activity in respect of clients or transactions to the firm’s MLRO;
* Avoiding discussing any potential or actual reports of suspicion with clients or any third parties (“Tipping off”)
* Referring any queries or requests from An Garda Siochana, Revenue, CAB or the FIU to the MLRO or Senior Management;
* Undertaking any AML-related training provided by the Firm;
* Keeping appropriate records of all AML related activity;
* Exercising extreme caution in relation to the acceptance of cash or the provision of firm’s client account details. All staff must adhere to policies in relation to cash and client accounts.
* Ensuring that they do not unwittingly commit the offence of money laundering by being alert to money laundering red flags.

**BUSINESS RISK ASSESSMENT SECTION:**

Section 54(3)(k) requires PCPs which detail internal systems and controls to identify emerging risks and keep business-wide risk assessments up to date.

The partners believe **(Firm Name)** is at a high/medium/low risk of being mis-used by clients to launder the proceeds of crime. This is based on the outcome of the firm’s Business Risk Assessment (attached) and the following factors:

* Types of Work undertaken – Mostly AML-regulated legal services/non-regulated legal services. Mostly Property? Litigation? Wills/Executry?
* Analysis of the typical client base and type of services provided
* High turnover of clients or a stable existing client base?
* High proportion of one-off clients/deals?
* Mostly face-to-face or non-face-to-face contact with clients?
* International element to the business - especially from non-EU countries with request to transfer funds to client account from accounts outside the EU
* Source of clients – referrals, walk-in or internet advertisement

Accordingly, our business risk assessment is summarised as follows:

(1) Client demographic is low risk because:

* a stable existing client base
* low turnover of clients
* meeting clients face-to-face is the normal practice
* clients normally resident in Ireland or very much connected with Ireland
* clients normally do not have complex ownership structures/trusts

The firm has controls in place to mitigate and manage potential departures from our typical low risk client demographic.

(2) Legal services are also low risk:

* non-complicated financial or property transactions/trusts
* it would be unusual for payments to be made to or received from third parties
* payments made by cash are rare
* transactions with a cross-border element are rare

The services we provide and our client base is relatively simple, involving few unusual services with most clients falling into similar categories.

The firm has controls in place to mitigate and manage potential departures from our typical low risk legal services.

**CUSTOMER RISK ASSESSMENT SECTION:**

Section 54(3)(a) requires every firm to have policies, controls and procedures (PCPs) relating to “identification, assessment, mitigation and management” of ML/TF risk factors.

In addition, section 54(3)(d) requires PCPs which enable the “identification and scrutiny of complex or large transactions, unusual patterns of transactions that have no apparent economic or visible lawful purpose and any other activity that the designated person has reasonable grounds to regard as particularly likely, by its nature, to be related to money laundering or terrorist financing.”

Section 54(3)(e) requires PCPs which include measures to be taken “to prevent the use for money laundering or terrorist financing of transactions or products that could favour or facilitate anonymity.”

Here, detail the firm’s approach/procedures for customer risk assessments, including

* Information from the Society’s 2018 Guidance “What does section 30B mean in practice for solicitors?” in Section 4
* Information about the firm’s customer risk assessment process or template (if applicable)
* Clarification that customer risk assessment and CDD is best undertaken before deciding to provide an AML-regulated legal service
* Who is responsible for risk assessment/how it is undertaken
* Detail the decision-making process, based on Customer Risk Assessment, around whether to provide an AML-regulated legal service and the extent of CDD measures to be applied
* When/How often reviewed
* High level overview of risk factors/“red flag indicators” for legal sector
* Control process for what happens when red flags/risks are identified before taking client on-board
* Detail about what happens when red flags/risks emerge during the provision of an AML-regulated legal service

**CUSTOMER DUE DILIGENCE PROCEDURES SECTION:**

Section 54(3)(b) requires PCPs which detail the firm’s CDD measures.

Here, detail firm’s procedures in relation to establishing identification and verification (ID&V), know your client (KYC), source of funds enquiries, ongoing monitoring etc.

* Who is responsible for establishing ID&V/how this is undertaken
* Timing of ID&V (NB the Society’s best practice guidance is to complete **all** CDD prior to deciding to provide an AML-regulated legal service)
* Types of CDD required depending on the Customer Risk Assessment outcome:

1. **Standard (Sections 33 and 35)**
2. Identifying the client and verifying the client's identity
3. Identifying the beneficial owners and taking measures reasonably warranted by the ML/TF risk to verify their identity
4. Obtaining information reasonably warranted by the risk of ML/TF on the purpose and intended nature of the business relationship
5. Conducting ongoing monitoring
6. **Simplified (section 34A)**

Section 34A permits simplified due diligence to be undertaken where the solicitor determines that the business relationship or transaction presents a low risk of money laundering or terrorist financing on the basis of specific statutory criteria.

1. **Enhanced (sections 37 and 39)**

The legislation prescribes the following four specific circumstances when enhanced due diligence measures must be applied:

1. Complex/Unusual transactions - Section 36A
2. Ascertain PEP status where there is a risk client is involved in ML/TF, then - Section 37

Detail the firm’s policies for identifying PEPs and measures to be applied (these will be dependent upon the outcome of the firm’s Business Risk Assessment and please see Section 5 of the 2018 Guidance for detailed information about PEPs)

1. Client is established or resides in a high-risk third country - Section 38A

Detail the firm’s policies for AML-regulated legal services where client is established or resides in a high-risk third country (please see Section 5 of the 2018 Guidance for detailed information about high-risk third countries).

1. Business relationship (client or AML-regulated legal service) is high risk for ML/TF - Section 39

**N.B.** The firm is cognisant of the Law Society’s recommendation that solicitors consider the extent to which they might unwittingly commit the substantive offence of money laundering by providing a high risk legal service which requires enhanced CDD measures. Solicitors should document their thought process and detail their KYC (knowledge of client) when determining whether to provide a high risk AML-regulated legal service. The exercise of ‘documenting your thought process’ when ML/TF red flags are present can greatly assist a solicitor in the future should an AML-regulated legal service ever be examined by an Investigating Accountant or investigated by the CAB or the FIU. See further the firm’s PCPs below about **ML/TF Risk Management Practices/Controls.**

**CDD Controls**

A firm’s CDD system can document:

* When CDD is to be undertaken
* Information to be recorded on client identity
* Information to be obtained to verify identity, either specifically or providing a range of options with a clear statement of who can exercise their discretion on the level of verification to be undertaken in any particular case
* When simplified due diligence may occur
* What steps need to be taken for enhanced due diligence
* What steps need to be taken, if ML/TF risk, to ascertain whether your client is a high-risk or low-risk PEP and subsequent controls that will be put in place
* When CDD needs to occur and under what circumstances delayed CDD is permitted
* How to conduct CDD on existing clients when it is necessary to do so and how often CDD information will be reviewed to ensure that it is up to date
* What ongoing monitoring is required

PCPs can include examples for staff of how the firm carries out its AML for different types of scenarios which shows the typical CDD life-cycle of 2 to 3 types of legal services.

**Reliance**

PCPs must cover reliance, which is discussed further in Chapter 7 of the 2010 Guidance Notes. A firm should consider including in their PCPs:

• the circumstances in which they consider it appropriate to rely on another regulated person, and

• the steps they will take when relying on another regulated person to satisfy themselves that they have complied fully with the requirements of the Regulations.

**Important information about reliance on others**

In relation to the legality of funds, the acceptance of funds by one designated body (e.g. a bank) is not necessarily an indication of the legality of those funds.  This is for a variety of reasons including the fact that once a report has been made there is the risk of the tipping off offence/offence of prejudicing an investigation (this precludes a person who has made a report from informing another person that a report has been made).

Chapter 7 of the 2010 Guidance Notes provides guidance in relation to third party reliance.   It is important to note that the fact that one designated entity (a third party) is carrying out its own CDD to meet its AML obligations, does not negate the need for any other designated person to carry out CDD to satisfy their own AML obligations. Accordingly, each designated person (whether a solicitor, or a financial or credit institution, etc.) involved in a transaction must carry out their own individual CDD to satisfy their AML obligations. The statutory AML obligations of a designated entity will not be satisfied by simply seeking and/or receiving any form of “confirmation” from another designated entity involved in a transaction.  Nor is any such practice envisaged under the AML legislation.  As per the AML legislation, each designated entity is required to fulfil their own statutory AML obligations, and it remains their responsibility and statutory obligation to do so, regardless of what other designated entities in a transaction may or may not be doing to meet their AML obligations.

**CASH & CLIENT ACCOUNT USE POLICY SECTION**

Here, detail Cash & Client Account Use Procedures adopted by the firm such as:

* The firm’s policy is to not accept cash (cash above a certain amount) for asset purchases
* The firm’s policy is to not accept cheques/transfers from persons other than a client or another solicitor into their client account (or the circumstances in which they will do so)
* The firm’s policy is to not provide client account details until after customer risk assessment, all CDD has been completed/decision to provide AML-regulated legal service has been made
* The firm’s policy is to not provide client account details for proposed transfers into client accounts from accounts outside of the EU
* The firm’s policy is to not provide client account details by email

The firm is mindful of the Society’s 2010 Guidance in relation to cash and client account use which is as follows:

“**Use of client accounts**

9.13     Client accounts should only be used to hold client money for legitimate transactions for clients, or for another proper legal purpose. Money-launderers will seek to route ‘dirty’ money through a solicitor's client account in order to ‘clean’ it, either by asking for the money to be returned or by purchasing a clean asset with the funds.

Why is it important to establish a policy on handling cash?

9.15    Clients may attempt to circumvent such a policy by depositing cash directly into a solicitor’s client account at a bank.  Solicitors should avoid disclosing client account details as far as possible and make it clear that electronic transfer of funds is expected.

9.16      If a cash deposit is received, a solicitor will need to consider whether there is a risk of money laundering taking place and whether it is a circumstance requiring a report to the authorities.

**Why is it important to monitor the sources of funds?**

9.17 Solicitors should monitor whether funds received from clients are from credible sources. For example, it is reasonable for monies to be received from a company if the client is a director of that company and has the authority to use company money for the transaction.

9.18    However, if funding is from a source other than the client, a solicitor may need to make further enquiries, especially if the client has not informed the solicitor what they intend to do with the funds before depositing them into the account. If a solicitor decides to accept funds from a third party, perhaps because time is short, he/she should ask how and why the third party is helping with the funding.

9.19   Solicitors do not have to make enquiries into every source of funding from other parties. However, solicitors must always be alert to warning signs and in some cases will need to get more information.

9.20     In some circumstances, cleared funds will be essential for transactions and clients may want to provide cash to meet a completion deadline. Solicitors should assess the risk in these cases and ask questions if necessary.

**Why is important to exercise care when disclosing client account details?**

9.21    Solicitors should think carefully before disclosing client account details.  Doing so could allow money to be deposited into the client account without their knowledge. If a solicitor  needs to provide client account details, he/she should ask the client where the funds will be coming from. Will it be an account in their name, from Ireland or abroad?  Solicitors should consider whether they are prepared to accept funds from any source about whom they have concerns.”

2018 Guidance from the Law Society provides:

“A good rule of thumb is to always be cautious of proposed legal services which will involve the routing of funds from outside of the EU into the EU financial system via a solicitor’s client account.  Solicitors must question the ML/TF risk posed by allowing their client account to be used as an entry point for money into the EU financial system.”

**ML/TF RISK MANAGEMENT PRACTICES/CONTROLS**

This section should detail

* the firm’s approach to mitigate the ML/TF risk they identified in their Business Risk Assessment
* how additional controls can be applied
* the level of personnel permitted to exercise discretion on the risk-based application of the AML legislation, and the circumstances under which that discretion may be exercised
* the CDD requirements to be met for simplified, standard and enhanced due diligence
* if outsourcing of CDD obligations or reliance will be permitted, and on what conditions
* the circumstances in which delayed CDD is permitted
* how you will restrict work being conducted on a file where CDD has not yet been completed
* when cash payments will be accepted
* when payments will be accepted from or made to third parties
* the manner in which ML/TF suspicions are to be dealt with in a firm

**Document your thought process if ML/TF red flags are present**

PCPs can include the following information about what to do when ML/TF red flags are present to ascertain the ML/TF risk - the approach of documenting your thought process to ascertain money laundering risk.

When red flag(s) are present, staff may find it helpful to document their thought process, this approach allows solicitors to place all relevant circumstances in context and follow the FATF’s (Financial Action Task Force) recommended method for interpreting red flags/indicators of suspicion which is as follows:

“…the methods and techniques used by criminals to launder money may also be used by clients with legitimate means for legitimate purposes. Because of this, red flag indicators should always be considered in context. The mere presence of a red flag indicator is not necessarily a basis for a suspicion of ML or TF, as a client may be able to provide a legitimate explanation. These red flag indicators should assist legal professionals in applying a risk-based approach to their CDD requirements of knowing who their client and the beneficial owners are, understanding the nature and the purpose of the business relationship, and understanding the source of funds being used in a retainer. Where there are a number of red flag indicators, it is more likely that a legal professional should have a suspicion that ML or TF is occurring.”

When red flag(s) are present, the firm may decide not to take on new instructions, and/or a solicitor may cease to act and/or a report may be statutorily required.

This is how the firm assesses and manages its money laundering and terrorist financing risk.

**ONGOING MONITORING SECTION**

Section 54(3)(c) requires PCPs relating to monitoring transactions and business relationships.

Section 54(3)(i) requires PCPs containing measures to keep documents and information relating to customers of that designated person up to date.

Please see ‘How can ongoing monitoring of the business relationship be conducted?’ in Section 5 of 2018 Guidance for detailed guidance.

In addition, section 54(j) requires PCPs which outline measures to be taken to keep documents and information relating to risk assessments up-to-date.

* This section should detail how, and at what frequency the firm undertakes ongoing monitoring of AML-regulated legal services/clients/business relationship
* This section can also address how the firm updates CDD for existing clients – see Section 1- 2018 Guidance.

**REPORTING ML/TF SUSPICIONS SECTION**

Section 54(3)(g) requires PCPs which detail reporting of suspicious transactions.

* The MLRO and/or Compliance Officer of the Firm is/are……
* They are responsible for….
* Scrutiny of unusual transactions highlighted by staff
* Deciding if a client can be taken on where there is a high risk of money laundering
* Reviewing suspicions from employees and deciding whether a report must be made

**Further detail in this section should include:**

* Detail how staff should make reports to the MLRO
* Make it clear obligations under the Act are mandatory – criminal offences
* Detail tipping off definition and potential issues
* What should be included in reports

PCPs can include detail about how suspicions are dealt with. For example, a PCP should require that comprehensive records of suspicions and reports are kept. These records may be necessary in the future in potential criminal proceedings and must be securely maintained due to their sensitivity/confidentiality. Such records may include notes of:

• ongoing monitoring undertaken and concerns raised by fee earners and staff

• discussions with the MLRO regarding concerns

• advice sought and received regarding concerns

• why the concerns did not amount to a suspicion and a disclosure was not made

• copies of any disclosures made

• correspondence with the Gardai/Revenue

• decisions not to make a report which may be important for the MLRO to justify his or her position to law enforcement agencies in the future

**MLRO/COMPLIANCE OFFICER RESPONSIBILITIES SECTION**

* The MLRO and/or Compliance Officer of the Firm is/are……
* In addition to dealing with reports of ML/TF suspicions, they are responsible for….
* Ensuring all staff are trained to a level appropriate to their role
* Reviewing the firm’s Business Risk Assessment and PCPs

Section 54(l) requires PCPs which provide for the monitoring and managing of compliance with and the internal communication of PCPs.

Firms must regularly review and update PCPs and maintain a written record of any changes made following such a review.

Firms must also maintain a written record of any steps taken to communicate your PCPs (and any changes) to staff.

Monitoring compliance will assist in assessing whether the PCPs that a firm has implemented are effective in identifying and preventing money laundering and terrorist financing opportunities within their practice.

Paragraph 10.9 of the Society’s 2010 Guidance suggests that a review for the purposes of monitoring effectiveness should cover the following issues:

1. Procedures to be undertaken to monitor compliance, which may involve:

• random file audits

• file checklists to be completed before opening or closing a file

• a compliance officer’s log of situations brought to their attention, queries from staff and reports made

1. Reports to be provided to senior management/MLRO on compliance
2. How to rectify lack of compliance, when identified
3. How lessons learnt will be communicated back to staff and fed back into the risk profile of the practice

Further detail can be provided here on how MLROs/Compliance Officers monitor and manage PCP compliance and communication:

**AML RECORD KEEPING SECTION**

Section 54(3)(h) requires PCPs which address record keeping.

Here, detail the record keeping procedures:

* How the firm manages, records and stores AML-related material, incl. retention period

Relevant records include:

* AML Policies, Procedures, Manuals
* Risk Assessments
* CDD/KYC material
* Evidence of staff training
* Suspicious Activity Reports

AML records must be kept for a minimum of 5 years (and no longer) after the relationship has ended or the transaction has been concluded.

See Chapter 11 of 2010 Guidance and ‘Reliance and record keeping’ in Section 3 of 2018 Guidance.

**AML TRAINING OF PARTNERS & STAFF SECTION**

Here, procedures could detail:

* A statement that all staff have been provided with Law Society Guidance to read
* 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 or emerging risk factors/new developments for the firm
* A note of training provided.

**RELATED DOCUMENTS SECTION**

Detail any internal firm documents, procedures which underpin/support the PCPs:

* *Business Risk Assessment*
* *Customer Risk Assessment Form*

*The Society accepts no responsibility for any compliance failures or loss incurred as a result of reliance on this example PCP. Solicitors’ firms must always ensure they are in compliance with all of their statutory AML obligations. The Law Society is grateful to the Law Society of Scotland on whose template PCP this sample document is based, adapted for the Irish legislative framework.*