HOUND & PORTER

FIND A HOUSE. MAKE IT HOME

Hound & Porter

AML & CTF Policy

Purpose	This document outlines AML & CTF for the Hound & Porter Estate Agent
Version & date:	V1 (February 2024)
Written by:	James Clancey (Consultant)
Reviewed by:	Christopher Nathan (Company Director)

Change Log

Version	Date	PIC	Update
v1.0	1/2/24		Version 1.0

Introduction

Hound & Porter Estate Agents (H&P) are a residential estate agent based at 58 Castle Walk, Reigate, Surrey, RH2 9PX.

This document defines the company policy for AML & CTF.

Purpose

This policy outlines H&P's approach to preventing and detecting money laundering and countering terrorist financing. H&P's UK's obligations under all applicable Anti-Money Laundering (AML) and Countering Terrorist Financing (CTF) legislation have been considered as part of this policy.

H&P is committed to deterring customers and outside parties from using the firm as a conduit for illegal activity. H&P has designed its program to provide a framework for effective compliance with laws and regulations, as well as to communicate its clear commitment to creating a strong compliance culture to the company's staff. The Directors recognise that their business can pose high inherent Money Laundering and Terrorist Financing (ML/TF) risk and that H&P needs commensurate Anti-Money Laundering/Counter-Terrorist Financing (AML/CTF) and Sanctions controls.

To ensure that H&P is compliant with relevant AML/CTF regulations, as a UK registered entity, the business undertakes robust mitigation measures that include the following:

- Has appointed a Money Laundering Reporting Officer (MLRO);
- Establishes a set of risk-based policies, procedures and internal controls;
- Conducts risk sensitive Due Diligence on all customers prior to onboarding;
- Undertakes ongoing monitoring of its customers' activities;
- Reports any suspicions of Money Laundering or Terrorist Financing to the MLRO. The MLRO has the authority to report suspicions to the National Crime Agency (NCA) as a Suspicious Activity Report (SAR);
- Assesses Money Laundering risks and applies enhanced due diligence measures in higher risk situations;
- Keeps appropriate and accurate records, as per the Money Laundering Regulations 2017 (as amended) (MLR 2017) requirements;
- Communicates new and any updates to policies and procedures to all H&P employees, connected persons and interested partners, in an efficient and timely fashion;
- Provides training on AML/CTF measures to all staff.

Any amendments made to relevant regulations or laws will result in this Policy being amended accordingly. The MLRO will then decide if it is appropriate to inform employees of these changes and any subsequent changes to their AML/CTF responsibilities.

This policy is approved by the Company Director and it is reviewed on an annual basis.

Scope

This policy applies to all H&P employees, contractors, consultants (hereinafter referred to as “staff”) whether conducted by staff or through outsourced service providers, and is intended to implement requirements defined by all applicable UK and European AML laws. It applies to those aspects of laws, regulations, controls, and procedures relating to:

- The Proceeds of Crime Act 2002 (PoCA);
- Money Laundering Regulations 2017 (as amended) (MLRs 2017);
- Money Laundering Regulations 2019 (as amended);
- Criminal Finances Act 2017;
- The Terrorism Act 2000 (TACT);
- Joint Money Laundering Steering Group Guidance (JMLSG); and
- Financial Conduct Authority (FCA) Handbook.

Breaches of this policy may be dealt with under disciplinary procedures and, in serious cases, could be treated as gross misconduct leading to summary dismissal.

Failure to comply by suppliers could result in contract termination.

Definitions

Money Laundering

Money Laundering (ML) is defined as engaging in acts designed to conceal or disguise the true origins of illegally derived proceeds, which includes cases of unlawful proceeds that appear to have been derived from legitimate origins or appear to constitute legitimate assets.

ML is defined as:

- The concealment or disguise of the true nature, source, location, disposition, movements, rights with respect to ownership of property knowing that such property is derived from an offence or offences or from an act of participation in such offences(s).
- The acquisition, possession or use of property knowing at the time of receipt that such property was derived from an offence or offence from an act of participation in such offence(s).
- The conversion or transfer of property, knowing that such property is derived from any offence or offences or from an act of participation in such offences, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an offence(s) to evade the legal consequences of his actions.

The most common sources of laundered money come from, but are not limited to;

- Illegal narcotics trade;
- Illegal arms trading;
- Sexual exploitation and prostitution;
- Corruption;
- Forgery;
- Armed robberies;
- Blackmail;
- Extortion;
- Arts and antique fraud;
- Fraud, including internet fraud;
- Smuggling;
- Tax fraud; and
- Human trafficking.

The typical stages of ML consist of:

Placement – Cash generated from criminal activities enters the financial system. Typically, this is in small amounts through cash or wire deposits from numerous other usually unrelated accounts or multiple deposits.

Layering – This money is then moved through a large number of transactions, typically with little or no real economic purpose, in order to hide the origin of the funds and to disguise ownership.

Integration – At the end of the process, the proceeds of the criminal activity will have all the appearance of legitimately earned wealth, which can then be integrated into the legal economy. This can be achieved through an investment into a business or in a work of art or other items of intrinsic value that can then be sold. Investment income of sale proceeds may now be repatriated back to the ultimate criminal beneficial owner.

Terrorist Financing

Whereas ML is the intention to disguise the true origin of funds, Terrorist Financing (TF) is the intention to disguise the funds' intended destination and subsequent usage, such as, for example, the financing of a terrorist's movement over a period of time, or funding specific terrorist attacks.

TF has included usage of sympathetic charities, criminal activities including drug trafficking, gun running and fraud. Additionally, with ISIS/Daesh having been forced out of previously held Syrian and Iraq locations, activities bearing hallmarks of traditional Money Laundering methods have been identified.

Funding for specific attacks have included the use of the unregulated Hawala banking systems which allows the anonymous movement of money between jurisdictions, physical importation of funds like traveller's cheques, wiring of funds between accomplices in different parts of the world using either their own accounts or the accounts of sympathisers.

Sanctions Screening

H&P recognises the responsibility it plays in the detection of prohibited financial activity by a sanctioned individual or entity. As such, H&P takes a zero-tolerance approach to any positive sanctions match it identifies. It also refuses to conduct business with anyone residing in a sanctioned country or with any sanctioned individual or business when it can be reasonably established that the match is genuine.

PEPs and Adverse Media Screening

H&P screens all customers/applicants, as well as the senior individuals aligned with the subject company (users, UBOs, directors, etc) against PEP lists and adverse media lists. Any alerts must be actioned appropriately and, when true matches are identified, a senior person (the MLRO) must make a determination as to whether a business relationship can be entered into (or, maintained for those already onboarded). If so, enhanced due diligence (EDD) measures must be applied, as set out in this Policy and further in the wider AML policy suite.

Nominated Officer/MLRO

H&P's Company Director is also the **Nominated Officer/MLRO** whose role is to ensure compliance with applicable rules, and to ensure the continued efficacy of internal systems and controls against ML. The MLRO has the appropriate level of authority within the firm to carry out their duties and responsibilities and has access to relevant and appropriate support, information, and training to carry out the designated role effectively.The MLRO is responsible for reviewing, approving and submitting Suspicious Activity Reports to the NCA.

The employees of H&P understand that questions with regards to the provisions contained within this Policy and/or any related procedures should be directed towards the MLRO.

The MLRO is responsible for pre-approving this Policy and maintaining a culture of compliance globally that supports adherence to AML/CTF regulations and applicable policies and procedures across the jurisdictions in which the business operates. The MLRO's responsibilities are outlined in further detail in the next section of this policy.

All H&P staff shall cooperate and work with the MLRO to provide them with unrestricted access to any business records, IT systems, or locations to which they request access for purposes of executing their duties. The staff shall also provide the MLRO with advance notice of all new products or changes to existing products that might affect the AML/CTF risk.

Responsibility of the MLRO

It is the role of the MLRO to ensure compliance with all applicable rules on systems and controls against ML. The MLRO has the appropriate independence and level of authority within the firm to carry out their duties and responsibilities and has access to the relevant and appropriate support, information and training to carry out their role effectively. The MLRO is responsible for core controls and systems used in the prevention and reporting of ML and TF.

The AML/CTF policies and methodology are appropriately created, monitored and documented measures to ensure ML risk is considered in relation to the:

- Development of new products;
- The onboarding of new customers;
- Changes in the H&P business profile;
- Appropriate AML (and other anti-financial crime) training is identified, designed, delivered and maintained to ensure that H&P staff are aware of and understand;
- Their legal and regulatory responsibilities and obligations;
- Their role in handling criminal property and terrorist financing;
- The management of the ML and TF risk;
- How to recognise ML and TF transactions and activities; and
- Understanding how to make internal SARs.
- Receiving and analysing SARs from H&P employees;
- Making external disclosures of SARs to the NCA;
- Responding to information requests from relevant authorities; and

Responsibility of all Employees

It is the responsibility of all H&P employees to co-operate with the MLRO in all aspects of this Policy.

Failure to comply with the Policy may result in termination of employment, and those individuals who knowingly commit or assist in ML or TF offences will be dismissed with cause and have contracts terminated with prejudice.

Employees are aware that under PoCA they are obliged to disclose to the MLRO when they “know or suspect” that another person is engaged in ML or where they “have reasonable grounds for knowing or suspecting” that a person is engaged in ML.

Employees are also aware of the risk they pose to themselves in the case of ‘tipping off’ a customer to any potential, pending, or on-going investigations as described in TACT is an offence under PoCA, and they will be personally liable for up to 5 (five) years imprisonment and an unlimited fine.

Employee ML obligations include:

- Sending a fully detailed SAR as soon as reasonably practical regarding suspicious activity or suspected or known money laundering to the MLRO.
- When informed that a specific transaction will take place at a certain point in the future and believing this transaction is suspicious, the employee will inform the MLRO immediately so that consent can be requested before the transaction can be carried out.
- Suspending any customer transaction and account should there be a suspicion of ML/TF.
- After submitting a SAR, they will not disclose to the customer that they are being investigated, or that a SAR has been submitted.
- Suspending any customer account should there be a name match on a name on HM Treasury’s Consolidated Sanction List, EU, OFAC or other such lists.
- Attending and completing the compulsory H&P AML/CTF training programme.
- All H&P staff shall comply with this Policy and facilitate its implementation.
- All employees and contractors of H&P are required to apply the requirements of this Policy in their daily activity and discharge their roles with utmost responsibility and consideration of this Policy requirements.
- The employees and contractors of H&P must attest to their understanding and adherence to this Policy through the annual mandatory reading.
- Responsibilities for specific controls are dependent on the job role and will be included in job descriptions.

Staff Performing Know-Your-Customer Officer (KYC)

Staff must conduct CDD and/or EDD on all customers and ensure compliance with H&P’s KYC requirements.

Risk Based Approach

A risk-based approach focuses on the nature, scale, and complexity of the underlying business. It allows H&P to identify potential risks of ML and TF, risk rate them, develop strategies to mitigate them and therefore focus resources where needed most within a defined tolerance level.

This approach determines the acceptable risks within the business, considering the nature of the customer, their transactions and the geographical regions in which the customers are based and conduct their activities.

The risk management and mitigation process consist of:

- Risk assessment of the customer profile;
- The implementation of risk mitigation controls;
- Maintaining a customer identification and beneficial ownership information (where applicable);
- Keeping all customer information up to date;
- Imposing greater vigilance and Enhanced Due Diligence (EDD) for certain customers and transactions; and
- Risk sensitive CDD review of the customer profile and activities.

Risk Sensitive Customer Due Diligence

Definition of a Customer

To the effect of this document, as well as other internal policies and procedures of H&P, we consider a “Customer” the following:

- any private person/individual or
- legal entity,
- who has successfully passed all the Know Your Customer and Due Diligence procedures established by H&P and with whom H&P has a business relationship as a party involved in the execution of a property transaction.

Customer Due Diligence

Customer Due Diligence (CDD) is the process where relevant information about the customer is collected and evaluated for any potential risk for the organisation or ML/TF activities. Simply put, CDD includes identification of the client and understanding their activities.

H&P will perform CDD on all of its clients:

- Before approving an account or executing any property transaction;
- When there is a suspicion of ML or FT;
- When there is any doubt about the veracity or adequacy of any information; and
- Periodically, according to the risk profile of the client.

Where H&P is unable to perform or complete any customer due diligence measures in relation to a customer, then it will:

- not establish a business relationship with the customer;
- terminate any existing business relationship with the customer; and
- consider whether it is required to file a suspicious activity report.

Initial CDD should include at least the following risk-sensitive measures to:

- identify the customer and if the customer is a company then identify the customer's beneficial owner(s) (the natural persons holding more than 25% of the shares either directly or indirectly), legal representatives, connected parties, individuals appointed to act on behalf of the customer, and individuals who have access to H&P's products;
- verify the names of the directors of the company;
- verify the customer's identity using reliable and independent sources and verify the beneficial owner's identity in such a way that H&P is satisfied that it knows who the beneficial owner(s) is;
- where no beneficial owners are identified, identify and verify the natural persons having executive authority for the customer;
- establish the purpose and intended nature of the business relationship;
- obtain information on the Client's management control structure and the nature of its business activity and source of funds.

Should an employee have any doubts regarding the document submitted for the CDD purposes, the employee shall refer to the MLRO who will assess the requirements applicable.

CDD is a fundamental control preventing H&P from becoming involved in ML or TF. By applying a risk-based approach, H&P ensures that it has a reasonable belief as to the identity of its customers and the identity of the beneficial owners, and sufficient awareness of the activity they are conducting through H&P.

H&P determines the extent of its CDD measures and ongoing monitoring on a risk sensitive basis. The firm considers numerous factors when assessing customer risk, including, but not limited to the following:

- Length of time owning the property & history behind the property
- Wether they have resided in the property and for how long
- Establishment within the local community and local business relationships
- If a business, years of operation;
- Shareholding layers and overly complex corporate structures;
- UBO & Directors, or individual, country of residence;
- Clarity of business model;
- Industry or employment background;
- Name screening results - PEPs, Adverse media, Sanctions;
- Country of registration;
- Legal entity type;
- Expected activity

The above risk factors are factored into the customer's profile risk assessment and, once documented, can evidence that the extent of these measures and the subsequent monitoring is appropriate in view of the ML and TF risks. Customers will subsequently be risk rated as low, medium or high risk.

The firm will keep the records of the customers' profiles with the associated ML/TF risks. The extent of the customer due diligence is inter-dependent on the customer's profile and associated risk with the enhanced due diligence applied to higher-risk customers.

The firm will keep the records of the customer profiles risk assessment with regular reviews and quality assurance conducted by the MLRO over the quality of the data.

H&P will conduct EDD with more intrusive questions and additional measures to assess the risks associated with its higher risk customers and expected transaction activity.

In any situations where the due diligence measures cannot be applied or where the EDD measures identify unacceptable ML/TF risk, the customer case/account will be rejected or closed.

The MLRO will file a SAR where sufficient evidence of suspicious activity is identified in this process.

Remote Identification of natural persons

Appropriate technology is consistently used in the UK to improve the customer onboarding experience while adequately assessing and managing money laundering and terrorism financing (ML/TF) risks. As a result H&P will use a Remote Identification process (also known as non-face-to-face identification) to verify the identity of natural persons (users, directors, UBOs etc), while recognizing that such process entails higher ML/TF risks. In order to combat the additional risks that arise from non-face-to-face business relationships H&P performs the below described process.

H&P will not use ID&V software. H&P will rely on customers supplying certified documents by an appropriate individual living in a low or medium risk location. The individual certifying must also be verifiable as appropriate to certify e.g. a regulated legal or accountancy professional etc.

Standard Customer Due Diligence

Standard Customer Due Diligence (CDD) (as detailed above in the customer due diligence section) is the minimum level of due diligence that H&P will undertake. Standard CDD may only be applied to low and medium risk clients as high risk clients are to be subjected to EDD (see below in the enhanced due diligence section). CDD shall include no less than the following:

1. Collecting information for the identification of the customer (& entity);
2. Collecting information for the identification of the users, directors and beneficial owners;
3. Verify the identification information (on both the entity and relevant individuals) with reliable and independent (third party) sources;

4. Screening the entity name and relevant individuals against sanctions, PEP, adverse media;
5. Establishing the purpose and intended nature of the business relationship;
6. Evaluating the risk profile of the customer.

Notwithstanding the above, if H&P has doubts about the veracity of the CDD information, or suspects that the applicant/customer may be connected with money laundering or terrorism financing, the Company shall conduct EDD or reject the application. We note that even after the application of EDD, these applicants/customers may be rejected.

Enhanced Due Diligence

All high-risk clients (identified as such through H&P's customer risk assessment) must be subject to enhanced due diligence (EDD) measures.

High risk clients are generally individuals or entities that are known to have an increased risk of being used by third parties for ML, TF purposes and/or are engaged in questionable activities that may expose H&P to legal, regulatory or reputational risk. It is very important to identify whether the client poses high risk early in the process. All such clients are subject to an in-depth analysis - EDD - of the risks related to the client and the nature of the client's business. The requirements for information and /or verification should in general be considered stricter for a high-risk client.

In addition to considering the output of the customer risk assessment, any applicants/customers with any PEP involvement identified, or with links to a high risk third country will be subjected to EDD measures.

Compulsory EDD measures:
H7P will perform the following enhanced measures for **all** high risk customers:

- Take reasonable measures to establish the source of wealth, and the source of funds of the customer;
- Identify and verify UBOs holding 10% or more of the shares and/or voting rights of the company (rather than >25% for low and medium risk customers);
- Each case will require a review and sign off by the MLRO;
- Collect additional documentation to verify the nature of business and source of funds of the customer and relevant persons, such as salary details, tax returns, bank statements, and external intelligence reports; and
- Conduct enhanced ongoing monitoring of the business relationship if the transaction takes an extended period of time, this is normally over 6 months from agreeing a sale to completing the transaction.

In addition to the above, when a PEP is identified, a PEP specific EDD Form must be completed – see **Appendix 1**.

In addition to the above and if decided on a case-by-case scenario the measures **may also include**:

- Obtaining information and documents from higher-risk clients, such as salary details, tax returns, bank statements;
- Requiring payments to be carried out through an account in the Client's name with another Financial Institution subject to similar or equivalent ML/FT due diligence standards,
- Using public sources of information (e.g. websites) to gain a better background (if any) of the client, and commissioning external intelligence reports (where it is not possible for 'H&P' to easily obtain information through public sources or where there are doubts about the reliability of public information);
- Extensive negative news and internet searches;
- Requiring additional forms of identification or certified documentation;
- Collection of additional information on the source of funds, wealth, and purpose of transactions;
- Reviewing the online activity of the prospective corporate customer and their directors/shareholders with Open-Source Investigation (OSINT);

MLRO approval of all high risk customers must be obtained if H&P wishes to establish or continue the relationship in the event if a customer is determined to be of an "unacceptable" ML/TF risk.

Unauthorised Access to H&P's Services

No access before CDD (at a minimum).
A customer shall not have access to any H&P service, and H&P shall not undertake any transaction for them, until the customer's identity has been verified, their risk profile determined, and reasonable assurance has been obtained that the client is not involved in any ML, FT or other suspicious activity.

No Suspicious Activity.
If H&P has reasonable ground for suspicion of a customer, whether existing or new, it shall:

- Put on hold any existing business relations with, or transactions for the customer;
- Not establish new business relations with, or undertake new transactions for, the customer; and
- File a SAR about individuals / entities for which there are reasonable grounds for suspicion.

Prohibited Clients

In addition, H&P shall not enter into business relationships with customer profiles presenting known ML, TF, or fraud risks.

H&P shall reserve the right to reject any other account that is not in line with the company's risk appetite.

Reporting Beneficial Ownership Discrepancies

Under Regulation 30A of the MLRs, H&P has an obligation to report to the registrar any discrepancy the firm finds during the onboarding process, or throughout the business relationship, relating to the beneficial ownership of the customer.

As H&P will use Companies House, among other KYB providers (such as Know Your Customer), to verify beneficial ownership information, H&P has implemented a procedure for reporting any known discrepancies to the registrar. These are further detailed in H&P's **CDD & Customer Onboarding Policy**.

Suspicious Activity Reports

Suspicion, as defined by the Courts, is a degree of satisfaction beyond mere speculation, which is based on some foundation, but which does not necessarily amount to belief. "Suspicion" is the third stage after "comfort" and "concern".

H&P has a legal duty to file SARs with the NCA under PoCA. All members of staff at H&P are regularly trained and fully aware of their obligation to report knowledge or suspicion of money laundering or terrorist financing to the MLRO as soon as reasonably possible. The MLRO will then decide whether it should then be reported to the NCA.

The following list is a non-exhaustive guide to some types of transactions that may be considered suspicious:

- Transactions that don't fit a customer profile;A customer exhibiting concerns regarding H&P Compliance and AML/CTF policies, particularly with respect to their identity;
- Reluctance or refusal of a customer to reveal information concerning business activities or unusual or suspect identification of business documents;
- False, misleading or incorrect source of funds information;
- Questionable customer background information
- A customer who is subject to news reports indicating possible criminal, civil or regulatory violations;
- A customer admitting or making statements about involvement in criminal activities.
- Repeated changes of a customer's address;
- The presence of an undisclosed principal, who the customer is reluctant to divulge information about;
- Confusing transaction details;
- Incomplete documentation;

- Multiple customer accounts that have similarities (transaction amounts, names, postal addresses);
- A customer requesting information on the process of SAR reporting;
- Changes of details to a transaction after a customer has been asked for documentation;
- A customer's occupation that is not in keeping with either the level or type of transactions being completed;
- Requests from a customer for funds to be delivered to a third party, where this may cause suspicion;
- The Compliance Director will keep a log of internal SAR escalations (submissions) and external SAR submissions. The MLRO will regularly review the SAR Log for quality assurance purposes.

Tipping Off

H&P prohibits all staff from "tipping off" customers that they are under investigation, or that H&P has filed a related SAR for.

It is an offence for a person "tip off" (i.e. inform) a person suspected of ML that:

- they or someone else has made a lawful disclosure (i.e. a SAR);
- there is a money laundering investigation taking place; or
- where the tipping off is likely either to prejudice any investigation arising from the disclosure or to prejudice the investigation disclosed to the person suspected of money laundering.

H&P also prohibits staff from practising "wilful blindness" by electing not to report unusual activity that they deem to be potentially suspicious.

The MLRO ensures that all employees receive training on these prohibitions and on how to escalate suspicious activity as part of the AML/CTF training program. Training must be undertaken and completed by all staff at least bi-annually, and more regularly as deemed necessary by the MLRO.

Ongoing Monitoring

Ongoing monitoring of relationships is required under the MLRs 2017. Further, financial transactions pose higher risks of ML and TF and require ongoing monitoring to detect suspicious transactions.

H&P will monitor customers and sale or purchases which occur over an extended period of time, where suspicions arise of where elevated risks have already been identified. This will involve H&P renewing or re-verifying aspects of a client prior to the completion of the transaction to ensure nothing material has changed and the risk profile is static.

Risk Review

H&P shall review a client's risk profile periodically if a review is triggered by an external event, including but not limited to, regulatory updates.

Dynamic Client Risk Rating

Dynamic client risk rating means that H&P will react and re-assess the risk score of a client as soon as material change is noticed (changes noticed during transaction monitoring, communication with the client etc.). The following is a non-exhaustive list of factors, that could trigger a full periodic KYC review:

A. **Client Risk factors**:

- Changes to majority ownership structure requiring identification of new Beneficial Owners and their risk profile of a company involved;
- Addition / exit of business activity of High-Risk countries; or
- Addition / exit of client Contractors/Suppliers from High-Risk Countries.

B. **Geographies**:

- Change of Place of incorporation / country of main business / country of funds receipt, destination / country of residence of the individuals or Beneficial Owner(s)/senior managers of a company.

C. **Screening**:

- Change in PEP status of the individuals or beneficial owners,

D. **Nature of relationship**:

- Cause to file SAR; or
- Record of suspicious transactions over a consecutive period

All potential reductions in existing client Risk Ratings are subject to MLRO approval.

Record Keeping

H&P will obtain and maintain accurate records relating to this Policy so that any interested regulatory body has access to records in a timely fashion, and these records are kept in such a way that they can be provided upon immediate request.

The retained records relate to:

- Customer due diligence and identity verification;
- SARs;
- Third party records;

- Customer files;
- Customer records relating to ongoing business relationships; and
- Records of transmissions made.

The MLRO ensures all AML/CTF records are maintained and filed according to H&P's policies as set out in the **Record Keeping Policy** and relevant legislation.

Additionally, with regards to our corporate customers, H&P will obtain no less than the following:

- copies of corporate or trust documents;
- regulatory authorisation (if applicable); and
- beneficial ownership information and identification information for all individuals authorised to provide instructions for the account, acting on behalf of the customer and/or owning the customer.

Training

One of the most important controls over the prevention and detection of ML is to have staff who are alert to the risks of ML/TF and well trained in the identification of unusual activities or transactions which may prove to be suspicious. This is especially important for staff who handle customer transactions or instructions. H&P's training programmes also cover temporary and contract staff carrying out such functions. H&P's training programme ensures:

- Employees are familiar with relevant AML/CTF and Sanctions requirements pertaining to their specific job functions;
- Management is knowledgeable regarding H&P's obligations and responsibilities under relevant AML requirements;
- An understanding of the significance of H&P's AML/CTF and Sanctions efforts and helps develop a strong culture of AML compliance across the company; and
- Vigilance throughout H&P to detect, escalate, and manage AML/CTF compliance-related risks as and when they arise.

The MLRO is responsible for developing a risk-based training program and ensuring that staff members in need of advanced training receive such training.

Appendix 1

Work Instruction for PEP Enhanced Due Diligence

PEP EDD Prepared By	
Is Client tagged/to be tagged a PEP	Yes No
Date of PEP EDD Review (dd/mm/yyyy)	
Client Entity Name	
PEP Relationship to Client:	Individual or UBO Controlling Person Director Authorised Person

1. PEP Status Determination		
1.	**Self-Declared Review** **Onboarding DD**	YES/NO YES/NO
2.	**Date of Identification (dd/mm/yyyy)**	
3.	**Date of Client Onboarding (dd/mm/yyyy)**	

2. PEP Details		
1.	**Full Name**	
2.	**PEP's most influential positions**	
3.	**Position Start Date and End Date (dd/mm/yyyy)**	

4.	**Elected or appointed political positions**	Elected Appointed N/A		
5.	**Country where position was held**		**Country Risk Rating**	High Medium Low
6.	**Country of residence**		**Country Risk Rating**	High Medium Low
7.	**Brief overview of other positions/politically exposed positions/Countries held**			
8.	**Does the PEP position held have a link to the entity's business and will help in the business success?**			
9.	**% of business growth derived or expected to be derived from government contracts or any form of engagement with the government.**			
10.	**PEP's Reputational record (indicate source, if any)**			
11.	**PEP's Family background**			
12.	**PEP's Source of Wealth (SoW - may**	Type of Source of Wealth		

	or may not be explicitly part of this entity's financials)	Source of Funds for investment in this entity, if this entity's ROI is the SoW Other Business ownership with Names of Companies, Countries of incorporation Employment Inheritance Investments sale proceeds Investment returns Property income Property Sales Others - Parent company is a listed entity on the Mongolian Stock Exchange. Based on (can be none, one, or all of the following) (in order of reliability): Supporting Documentation received (e.g. Sale deeds, Settlement deeds, IT Filings, Work experience, last drawn salary slip, etc) Information gathered on-line from reliable reporting Bank Statement Self-declared in public materials Self-declared to H&P, including through auditor / accountant Information gathered online from unreliable sources

3. Screening Results		
1.	***Name Screening Results on PEP***	(i) Materiality identified Yes No (ii) Materiality category (if yes) High Medium Low
2.	***Name screening results on Customer Entity***	(i) Materiality identified Yes No (ii) Materiality category (if yes) High

		Medium Low
3.	***Is the customer a PEP***	Yes No

Appendix 2

iSAR Template

{Business Name}

Raised by: Name, Team
Raised on: Date

EXECUTIVE SUMMARY

Client Profile	Individual or Business Name: Signed up on: Transaction Amount: Account Manager: -
Executive Summary	Documents in line with transaction: No/Yes - Description Counterparties in line with activity: No/Yes - Description Transaction in line with activity: No/Yes - Description Sanctions identified: No/Yes - Description Explanation from Client: No/Yes - Description
Knowledge or suspicion of ML/TF	Describe your knowledge or suspicion
Linked Acts	List linked accounts
Initiated by	H&P or name of partner
Suggested Mitigation	*Select your suggestion & delete other options* Close H&P Account Freeze H&P Account Close Partner Services (Partner Name(s)) Keep Open
Risk & Compliance Committee Decision	TBC

BACKGROUND DETAILS

Background of Individual or Main User:

Describe the user, nationality, profile, address, etc.

Background of Business:

Describe the business, location, business activity, address, etc.

AML INVESTIGATION

Research and Analysis:

Detailed analysis of the investigation, including screenshots if applicable

Explanation by Client:

Questions asked to client & explanations provided
(Mandatory to clarify except if AML hit)

Linked Accounts (if any) (other accounts linked to Director/ UBO/Admin users)

Explain link

Conclusion:

Conclusion of the investigation

Recommendation:

Recommendation & proposed next step