Anti- Money Laundering & Terrorist Financing Policy

ANTI- MONEY LAUNDERING & TERRORIST FINANCING POLICY

Department	**Academic Registry**	**Document No.**	**S16**
Document Type	**Anti- Money Laundering & Terrorist Financing Policy**	**Revision**	**2**
Owner	**Academic Registry**	**Pages**	**12**
Relevant to	**All OU Faculty and Students**		
Prepared by	**President and Executive Board Member** **Project and Compliance Lead**		
Reviewed by	**President and Executive Board Member** **Head of Student Experience and Academic Registry** **Project and Compliance Lead**		
Approved by	**President and Executive Board Member**		
Date Introduced	**1st September 2025**		
Custodian	**Academic Registry**		

Revision History

Revision No.	Revision Date	Section No.	Remarks
1.0	August, 2022		New Document
2.0	August, 2025	All Sections	Updated

Dissemination

Through OU Student Support Service Portal and website to all OU students and staff.

Internal Control and Validation

To ensure compliance with this policy and procedure:

- The Dean, Academic Affairs is responsible for the implementation.
- The Academic Registry will maintain control and compliance.

TABLE OF CONTENTS

1.1. Purpose and Objective

1.1.1. The purpose of this document is to make all OU Staff, Administrators, Contractors of the University aware of the strict money laundering policy that Oryx University (the University) follows.

1.1.2. The University is committed to the highest standards of openness, transparency, accountability, and to conducting its affairs in accordance with the requirements of the relevant funding and regulatory bodies. The University has a zero-tolerance approach to money laundering.

1.1.3. This policy sets out the respective obligations of the University and its staff. It also sets out the procedure to be followed if money laundering is suspected and defines the responsibility of individual employees in the process.

1.2. Scope

1.2.1. This policy applies to the University and all those working for it, whether as an officer, employee, worker, intern, secondee, subcontractor, administrator, agent or in any other capacity (for the purposes of this Policy, collectively referred to as "Staff").

1.2.2. Any failures to adhere to this policy may be dealt with under the University's Staff Policies as appropriate. Note that any such failures also expose the individual concerned to the risk of committing a money laundering criminal offence.

1.3. Definitions

Money Laundering	The process of taking profits from crime and corruption and transforming them into legitimate assets.
Terrorist Financing	The collection or provision of funds for terrorist purposes and hide the funding activity and the financial channels used.
Offence	Constitutes a person's benefit from criminal conduct or any property that, directly or indirectly, represents such a benefit (in whole or partly) where the person concerned knows or suspects that it constitutes or represents such a benefit.

1.4. Abbreviations

OU	Oryx University
PEP	Politically Exposed Persons
SAR	Suspicious Activity Report
KYC	Know Your Customer

1.5. Money Laundering Warning Signs or Red Flags

1.5.1. Payments or prospective payments made to or asked of the University can generate a suspicion of money laundering for a number of different reasons. For example:

1.5.1.1. large cash payments.
1.5.1.2. multiple small cash payments to meet a single payment obligation.
1.5.1.3. payments or prospective payments from third parties, particularly where there is no logical connection between the third party and the student, or
1.5.1.4. where the third party is not otherwise known to the University, or
1.5.1.5. where a debt to the University is settled by various third parties making a string of small payments
1.5.1.6. payments from third parties who are foreign public officials or who are politically exposed persons ("PEP")
1.5.1.7. payments made in an unusual or complex way
1.5.1.8. unsolicited offers of short-term loans of large amounts, repayable by cheque or bank transfer, perhaps in a different currency and typically on the basis that the University is allowed to retain interest or otherwise retain a small sum
1.5.1.9. donations which are conditional on particular individuals or organisations
1.5.1.10. who are unfamiliar with the University, being engaged to carry out work
1.5.1.11. requests for refunds of advance payments, particularly where the University is asked to make the refund payment to someone other than the original payer
1.5.1.12. a series of small payments made from various credit cards with no apparent connection to the student and sometimes followed by chargeback demands
1.5.1.13. the prospective payer wants to pay up-front a larger sum than is required or otherwise wants to make payment in advance of them being due
1.5.1.14. prospective payers are obstructive, evasive, or secretive when asked about their identity or the source of their funds or wealth or reason for payment
1.5.1.15. prospective payments from a potentially risky source or a high-risk jurisdiction

1.5.1.16. the payer's ability to finance the payments required is not immediately apparent or the funding arrangements are otherwise unusual

1.5.1.17. An individual or company attempts to engage in "circular transactions" where a payment is made to the University followed by an attempt to obtain a refund

1.5.1.18. A person or company undertaking business with the University fails to provide proper paperwork (examples include charging taxes but failing to quote a tax number or invoices purporting to come from a limited company, but lacking company registered office and number)

1.5.1.19. A potential supplier submits a very low quotation or tender. In such cases, the business may be subsidised by the proceeds of crime with the aim of seeking payment from the University in "clean money".

1.5.1.20. Involvement of an unconnected third party in a contractual relationship without any logical explanation.

1.5.2. This list is not exhaustive, and money laundering can take many forms. If there are any concerns, then these should be raised with the **Nominated Officer** – A person who is appointed by the management of OU and will work closely with them in regard to all matters relating to suspicious of money laundering.

1.6. Domain of Implementation

1.6.1. The University has appropriate procedures in order to minimise the risk of money laundering also the University will:

1.6.1.1. conduct an annual risk assessment to identify and assess areas of risk money laundering and terrorist financing particular to the University;

1.6.1.2. implement controls proportionate to the risks identified;

1.6.1.3. establish and maintain policies and procedures to conduct due diligence on funds received;

1.6.1.4. review policies and procedures annually and carry out on-going monitoring of compliance with them;

1.6.1.5. appoint a Nominated Officer to be responsible for reporting any suspicious transactions to the relevant law enforcement officers of the State of Qatar;

1.6.1.6. provide training to all relevant members of staff, including temporary staff, on joining the University, and provide annual refresher training; and

1.6.1.7. maintain and retain full records of work done pursuant to this policy.

1.7. Roles and Responsibilities

1.7.1. **Vice President - Operations** has responsibility for the Anti- Money Laundering & Criminal Finances Act of the UK and , which will be reviewed by the **Board of Trustees**. The Vice President - Operations will ensure:

1.7.1.1. annual (more frequently if circumstances change) assessments of the University's money laundering and terrorist finance risks are conducted and relied on to ensure the effectiveness of this policy;

1.7.1.2. appropriate due diligence is conducted, as a result of which risks relating to individual transactions are assessed, mitigated, and kept under review;

1.7.1.3. anti-money laundering and counter-terrorist finance training is delivered within the University, including training on this policy, with records of attendance maintained; and

1.7.1.4. this policy is kept under review and up-dated as and when necessary and levels of compliance are monitored

1.7.2. To facilitate the review and accountability functions, the Vice President of Operations will ensure:

1.7.2.1. the availability of appropriate management information to permit effective oversight and challenge; and

1.7.2.2. the maintenance and retention of full records of work done under this policy. The University will retain all anti-money laundering and counter-terrorist finance records securely for a period of at least five years.

1.7.3. **Nominated Officer** is the primary contact for any further information or to report any suspicious activity. The Nominated Officer is responsible for:

1.7.3.1. receiving reports of suspicious activity;

1.7.3.2. considering all reports and evaluating whether there is – or seems to be, any evidence of money laundering or terrorist financing;

1.7.3.3. reporting any suspicious activity or transaction to the local law enforcement officer by completing and submitting a Suspicious Activity Report;

1.7.3.4. asking the local law enforcement officer for consent to continue with any transactions that must be reported and making sure that no transactions are continued illegally.

1.7.3.5. Recording in writing the reasons for their decision and retain that record centrally. Information that an authorised disclosure has been made must never be kept on the file relating to the person concerned.

1.7.4. **Staff** - All Staff are responsible for reporting suspicious activity:

1.7.4.1. Money laundering legislation applies to all staff

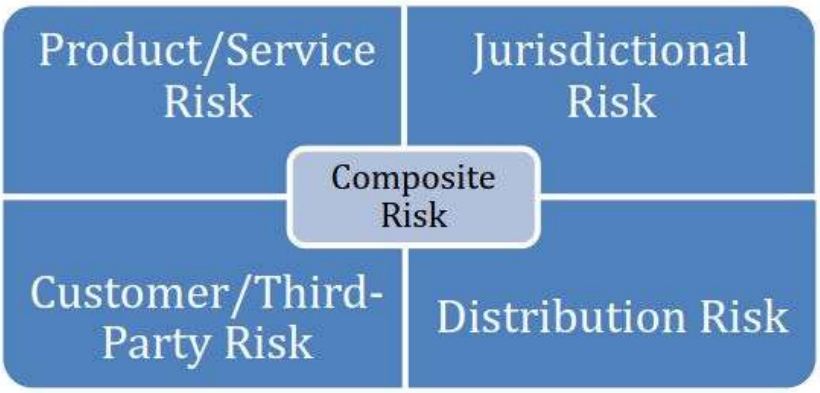
1.7.4.2. Staff who need to report suspicious activity must complete the Suspicious Activity Report (SAR) which is detailed in **Appendix 1.**

1.7.4.3. Staff could commit an offence if they suspect money laundering (or if they become involved in some way) and do nothing about it.

1.7.4.4. Staff should provide as much detail as possible and the report must be made in the strictest confidence, being careful to avoid "tipping off" those who may be involved.

1.8. Risk Assessment

1.8.1. A risk assessment will be performed at a minimum annually, and more frequently circumstances should change. The risk assessment will consider 4 main areas.



1.8.1.1. **Product / Service Risk** is the risk associated with delivery of University activity including teaching, research, enterprise, and conferencing activity.

1.8.1.2. **Jurisdictional Risk** is the risk associated with the University' countries of operation, location of students and customers, suppliers, and agents.

1.8.1.3. **Customer/Third-Party Risk** is the risk associated with the people and/or organisations that we undertake business with including customers/third-parties, beneficial owners, agents, contractors, vendors, and suppliers. Politically Exposed

Persons (PEP's) and Sanctioned Parties are also considered within this risk.

1.8.1.4. **Distribution Risks** is the risk associated with how we undertake business, including direct and indirect relationships (e.g., via an agent or third-party), face-to-face, digital/online, and telephonic.

1.9. Know Your Customer (KYC)

1.9.1. Anti- Money Laundering Regulations requires that the University must be reasonably satisfied as to the identity of the customer (and others) that they are engaging with in a contractual relationship.

1.9.2. To discharge the "reasonably satisfied" requirement the University must obtain a minimum level of personal information from a customer including date of birth and home address. For third parties, letters or documents proving name, address and relationship should be obtained.

1.9.3. If an organisation is not known to the University, then letter-headed documents, website and credit checks should be undertaken as appropriate.

1.9.4. The University must be clear on the purpose and the intended nature of the business relationship i.e., knowing what you are doing with them and why. This is why it is important for staff to comply with this policy (and other applicable policies) when engaging with any third party on behalf of the University.

1.10. Politically Exposed Persons (PEP) Checks

1.10.1. A **politically exposed person (PEP)** is someone who has been appointed by a community institution, an international body or a state, including the UK, to a high-profile position within the last 12 months.

1.10.2. Under anti-money laundering regulations, the main aim of applying additional scrutiny to work involving PEPs is to mitigate the risk that the proceeds of bribery and corruption may be laundered, or assets otherwise stripped from their country of origin. PEPs can be:

1.10.2.1. heads of state

1.10.2.2. heads of government, ministers, and deputy or assistant ministers

1.10.2.3. members of Parliament

1.10.2.4. members of courts of auditors or of the boards of central banks

1.10.2.5. ambassadors and high-ranking officers in the armed forces

1.10.2.6. members of the administrative, management or supervisory bodies of state-owned enterprises

1.10.2.7. members of supreme courts, constitutional courts, or other high-level judicial bodies whose decisions are not generally subject to further appeal, except in exceptional circumstances

1.10.3. PEPs also include:

1.10.3.1. the person's family members

1.10.3.2. close business associates

1.10.3.3. beneficial owners of the person's property (someone who enjoys the benefits of ownership even though the title of the property is in another person's name)

1.10.4. The University will use information that's reasonably available to help identify PEPs, including:

1.10.4.1. public domain information, such as parliament and government websites

1.10.4.2. reliable public registers,

1.10.4.3. commercial databases that contain lists of PEPs, family members and known close associates

1.11. Refunds

1.11.1. The University will undertake appropriate checks before processing any refunds:

1.11.1.1. Funds can only be refunded back to the original payer

1.11.1.2. Funds cannot be refunded to any third party

1.11.1.3. Funds once received from bank or cash by hand cannot be refunded as cash

1.11.1.4. Where the original payment has been received from abroad the refund will be to the foreign bank account only

1.11.1.5. Where the original payment has been received from local bank the refund will be to the local bank account

1.11.1.6. The University does not refund any money in cash irrespective of the total amount

1.12. Training

1.12.1. On joining the University any staff whose duties include undertaking a finance function will receive anti-money laundering training as part of their induction process.

1.12.2. Staff undertaking a finance function undergoes annual refresher anti-money laundering and counter-terrorist finance training.

1.12.3. The University's anti-money laundering and counter-terrorist financing training will include the applicable law, the operation of this policy and the circumstances in which suspicions might arise.

1.13. Advice and Information

1.12.1. The OU Academic Registry Staff are available to advise on matters about money laundering, precautions, concerns about financing, etc. procedures. If anyone wishes to contact, they can do so at Academic Registry.

1.12.2. Information on this Policy is available on the University's Webpages at https://www.oryx.edu.qa/policies/ or by contacting the Academic Registry via telephone numbers +974 4021 0000 or via email at registry@oryx.edu.qa.

1.12.3. Further information and contact details are also available on the University Web pages at https://www.oryx.edu.qa/.

1.14. Appendix

Appendix: Suspected Money Laundering Reporting Form

CONFIDENTIAL - Suspected Money Laundering Reporting Form	
Please complete and send this (in a physical format) to the Nominated Officer using the details below	
From:	**Department/Service:**
Contact Details:	
DETAILS OF SUSPECTED OFFENCE [Please continue on a separate sheet if necessary]	
Name(s) and address(es) of person(s) involved, including relationship with the University:	
Nature, value, and timing of activity involved:	
Nature of suspicions regarding such activity:	
Details of any enquiries you may have undertaken to date:	
Have you discussed your suspicions with anyone? And if so, on what basis?	
Is any aspect of the transaction(s) outstanding and requiring consent to progress?	
Any other relevant information that may be useful?	
Signed:	**Date:**
Contact details: **Job title:** Vice President - Operations **Address:** **Al Rayyan Campus, Doha, Qatar** **Email Address:** mafeel@oryx.edu.qa	
Please do not discuss the content of this report with anyone you believe to be involved in the suspected money laundering activity described. To do so may constitute a tipping off offence, which may carry a penalty and/or imprisonment and/or an unlimited fine as per the law of State of Qatar.	