University of Strathclyde

Anti-Money Laundering Policy

Version 1, Publication Date 21 Oct 2025

Contents

1. Introduction

The University is committed to the highest standards of ethical conduct and integrity in its business activities in the UK and overseas. It will therefore ensure that it has in place proper, robust financial controls so that it can protect its funds and ensure continuing public trust and confidence in its activities. Some of those controls are intended to ensure that the University complies in full with its obligations not to engage or otherwise be implicated in money laundering or terrorist financing. This Anti-Money Laundering Policy (Policy) outlines how the University and associated individuals will manage money laundering risks and comply with legal obligations. Associated individuals in the context of this Policy includes, but is not limited to, all staff, students, applicants, agents, volunteers, lay members, subsidiary companies of the University and to third parties, including academic partners, undertaking business on behalf of the University and its subsidiary companies.

The key elements of the UK anti-money laundering legislative and compliance framework (Money Laundering Framework) that apply to UK universities are listed in Appendix I. For the purposes of this Policy, money laundering will be considered as any activity which breaches any of the terms of the Money Laundering Framework. Key terms used in this Policy are defined in Appendix 5, Definitions.

Other relevant University policies that should be read in conjunction with this Policy are:

- Financial Regulations
- Fraud Policy
- Treasury Management Policy
- Public Interest Disclosure (Whistleblowing) Policy
- Anti-Bribery and Corruption Code of Conduct
- Policy for the Offering or Receipt of Gifts, Hospitality and Other Benefits

2. Scope and Purpose

This Policy applies to all University activities undertaken in the UK or overseas. Associated individuals could be committing an offence under the Money Laundering Framework if they suspect money laundering or if they become involved in some way and do nothing about it. This would include failing to report suspicious activity.

This Policy outlines the University's arrangements to comply with the five key requirements of the Money Laundering Framework which are:

- All organisations must obtain satisfactory evidence of the identity of each customer with whom it deals with and/or has a business relationship;
- This evidence of client identity must be retained for the duration of the client relationship and for a period of five years after it terminates or in line with the University Record Management Policy (Records Management Policy); details of transactions must be kept for the same period;
- Any suspicious transaction, whether in connection with a new or existing client, must be reported immediately to the Money Laundering Reporting Officer (MLRO);

- The MLRO must, if deemed appropriate, report suspicion of money laundering to the appropriate authorities in the relevant jurisdiction. In the UK this is the National Crime Agency (NCA);
- Appropriate training must be provided to all relevant individuals who handle, or are responsible for handling, any transactions with the organisation's clients and counterparties to ensure that they are aware of the organisation's procedures which guard against money laundering and the legal requirements of the Money Laundering Framework.

This Policy enables the University to comply with its legal obligations and sets out the procedure to be followed if money laundering is suspected and defines the responsibility of both the University and relevant individuals in the process.

The University has a zero-tolerance approach to money laundering and serious action will be taken against anyone found to be involved in money laundering.

Where suspected money laundering is associated with activities undertaken through University of Strathclyde Students' Association (USSA), the University will work with USSA in line with relevant USSA policies.

3 What is Money Laundering?

Money laundering is the process of taking profits from crime ('dirty funds') and transforming ('sanitising') them into legitimate assets. This process conceals the true origin or ownership of the funds, and so 'cleans' them. It also covers money, however come by, which is used to fund terrorism (reverse money laundering).

Money laundering schemes come with varying levels of sophistication from the very simple to the highly complex and can be carried out in any part of the world. Straightforward schemes can involve cash transfers or large cash payments whilst the more complex schemes are likely to involve the movements of money across borders and through multiple bank accounts.

Although money laundering is a single process, it can be broken down into three stages:

i) Placement – the process of getting criminal money into the financial system and hiding its source;

ii) Layering – the process of moving the money within the financial system through layers of transactions which makes it more difficult to detect and uncover laundering activity; and

iii) Integration – the process whereby the money is finally integrated into the economy, perhaps in the form of a payment for a legitimate service.

4 Principal Money Laundering Offences

Appendix 1 sets out the Money Laundering Framework applicable to UK Higher Education Institutions. The three main types of offences in the UK which apply to universities are as follows:-

I. Direct activities, or 'Principal offences'

These offences come under the Proceeds of Crime Act 2002

II. Prejudice of investigations

These offences also come under the Proceeds of Crime Act 2002

III. Failure to report a suspicion

5 Proceeds of Crime Act 2002 (POCA)

A key part of the Money Laundering Framework is the Proceeds of Crime Act 2002 (POCA) which sets out three main offences relating to any property, for example, cash, bank accounts, or any other assets, that an individual benefits from and which they know, or suspect, comes from criminal conduct. Any property which meets this definition is called criminal property.

It is a crime, punishable by up to fourteen years imprisonment, to:

- conceal, disguise, convert or transfer criminal property, or to remove it from the United Kingdom (POCA s327)
- enter into an arrangement that you know, or suspect makes it easier for another person to acquire, retain, use or control criminal property (POCA s328);
- acquire, use or possess criminal property when adequate consideration (i.e. proper market price) is not given for its acquisition, use or possession (POCA s329).

Associated individuals can commit these offences when handling or dealing with any payments to the University arising from criminal activity and there is no minimal value. If an individual makes or arranges to make a repayment of funds originating from criminal conduct, they risk committing the first two of the above offences under the POCA, and if they accept a payment, they risk committing the third offence under the POCA.

Motives for the prohibited act are irrelevant, and no motive overrides the criminal law. For example, processing a refund so that the University is not retaining suspicious funds, or accepting the suspicious fund knowing the student was a victim and it is in their best interest would not negate the money laundering offence. Criminal liability does not expire no matter how long ago the criminal conduct to generate the criminal property, or the money laundering offence itself took place.

With all three offences, there is a defence if there has been a disclosure of the transaction to the MLRO at the University and an 'authorised disclosure' to the National Crime Agency (NCA). An authorised disclosure is a Suspicious Activity Report (SAR) that is submitted to the NCA.

A Defence Against Money Laundering (DAML) SAR can be requested from the NCA where a reporter knows or suspects that they will be dealing with criminal property in a way that may amount to a principal offence under the POCA. An example would be requesting consent to refund a £5,000 student deposit due to suspicion that the payment has been made by a stolen card. Requests for consent must be made for each transaction; these cannot be hypothetical or general.

It is a crime, punishable by up to five years imprisonment, for a MLRO who knows or suspects money laundering or who has reasonable grounds to know or suspect it, having received a disclosure not to make an onward authorised disclosure to the NCA as soon as practicable after they received the information.

Section 12 of this policy sets out how disclosures to the MLRO are to be made.

The purpose of making an authorised disclosure to the NCA is to allow the NCA to investigate the suspected money laundering so it can decide whether to refuse consent to the transaction. That investigation would be compromised if the person concerned (or indeed anyone else) were to be told that an authorised disclosure had been made. To prevent this happening Section 342 of the POCA provides that it is a crime, punishable by up to five years imprisonment, to make a disclosure which is likely to prejudice the money laundering investigation. This means you could potentially commit an offence if you inform or 'tip-off' a student about whom you have raised a SAR. **This policy requires all SARs to the NCA to be kept strictly confidential.**

6 The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017)

MLR 2017 are aimed at protecting the gateway into the financial system. The regulations apply to a range of businesses all of which stand at that gateway, and they require these businesses to conduct

money laundering risk assessments and to establish policies and procedures to manage identified risks. Businesses to which the regulations apply are specifically required to conduct due diligence of new customers; a process known as Know your Customer ("KYC"). There are criminal sanctions, including terms of imprisonment of up to two years, for non-compliance. Whilst the University is not covered by MLR 2017 in its work as a provider of education, the regulations provide a guide in the management of risk in handling money. Under this Policy, due diligence is at the heart of the University's approach to managing risk.

7 Terrorist Finance – The Principal Terrorist Finance Offences

Whereas money laundering is concerned with the process of concealing the illegal origin of the proceeds of crime, terrorist financing is concerned with the collection or provision of funds for terrorist purposes. The primary goal of terrorist financers is to hide the funding activity and the financial channels they use. Therefore, the source of the funds concerned is immaterial, and it is the purpose for which the funds are intended that is crucial.

Payments or prospective payments made to or asked of the University can generate a suspicion of terrorist finance for several different reasons, but typically might involve a request for a payment, possibly disguised as a repayment or reimbursement, to be made to an account in a jurisdiction with links to terrorism.

Sections 15 to 18 Terrorism Act 2000 create offences, punishable by up to 14 years imprisonment, of:

- raising, possessing or using funds for terrorist purposes;
- becoming involved in an arrangement to make funds available for the purposes of terrorism; and
- facilitating the laundering of terrorist money (by concealment, removal, transfer or in any other way).

These offences are also committed where the person concerned knows, intends or has reasonable cause to suspect that the funds concerned will be used for a terrorist purpose.

In the case of facilitating the laundering of terrorist money, it is a defence for the person accused of the crime to prove that they did not know and had no reasonable grounds to suspect that the arrangement related to terrorist property.

Section 19 Terrorism Act 2000 creates an offence, punishable by up to five years imprisonment, where a person receives information in the course of their employment that causes them to believe or suspect that another person has committed an offence under sections 15 to 18 of Terrorism Act 2000 and does not then report the matter either directly to the police or otherwise in accordance with their employer's procedures. This Policy sets out those procedures at section 14 below.

8 The Offence of Prejudicing Investigations

Section 39 Terrorism Act 2000 creates an offence, punishable by up to five years imprisonment, for a person who has made a disclosure under section 19 Terrorism Act 2000 to disclose to another person anything that is likely to prejudice the investigation resulting from that disclosure. **This policy requires disclosures to be kept strictly confidential.**

9 University Responsibilities

The University adopts a risk-based approach towards anti-money laundering and conducting due diligence. Whilst much of the University's financial activities could be considered relatively low risk from the perspective of money laundering, the University, its subsidiary companies and all associated individuals of the University and its subsidiary companies need to be vigilant against financial crime and risks that the University faces. Instances of suspected money laundering are likely to be rare at the University, but we

must be aware of the Money Laundering Framework.

MLR 2017 requires the University to undertake a risk assessment and to demonstrate and document that it was carried out and has been/will be kept up-to-date. The Finance Directorate has responsibility for the Risk Assessment and it is owned by the MLRO. There are four main risk areas to review and these are listed in Appendix 2 along with examples of money laundering warning signs or “red flags”.

To manage the University’s risk of money laundering the University has:

- Ensured this Policy is proportionate to the specific risks identified.
- Implemented internal systems, policies, controls and procedures to address money laundering and terrorist financing risks identified through the risk assessment.
- Identified external controls including the banks who monitor and prevent transactions with sanctioned regimes.
- Agreed customer due diligence procedures for transacting with students, customers and third parties.
- Appointed a MLRO to receive, consider and report as appropriate, disclosure of suspicious activity.
- Implemented a procedure to enable the reporting of suspicious activity.
- Maintained adequate records of transactions; and
- Undertaken appropriate awareness raising and training.

10 Protecting Students

Legislation in the area of money laundering is complex and students and applicants can be at risk of money laundering because they may be targeted by criminals who exploit their lack of knowledge of the activity. Criminals may use students as "money mules" to move money or to purchase bank accounts and identification details.

How students can be targeted:

- Fake job adverts: Criminals may lure students into laundering money with fake job adverts that offer easy money
- Social media and chat forums: Criminals may target students on social media and chat forums
- Face-to-face contact: Criminals may target students face-to-face

The University will focus on the training and education of staff and students to protect students against these risks.

11 Customer/Collaborator Due Diligence

Customer due diligence (CDD) is the process by which the University assures itself of the source of funds it receives and that it can be confident that it knows the people and organisations with whom it works. MLR 2017 requires that the University must be reasonably satisfied as to the identity of the customer (and others) with whom they are engaging in a business relationship. Therefore, the University has policies and procedures for performing CDD, and transaction monitoring arrangements on a risk-managed basis with systems and controls in place to mitigate any financial crime risks.

Our customer due diligence follows the principles of Know Your Customer (KYC), one of the fundamental precepts of global anti-money laundering regulations. This due diligence process ensures the identity of a new customer must be established before a business or financial relationship can begin or proceed.

The three components of KYC are:

1. Ascertaining and verifying the identity of the customer/student and confirming this by obtaining documentary evidence that is independent and reliable. In order to satisfy the requirements, identity checks are interpreted as obtaining a copy of photo- identification (such as a passport) and proof of

address (such as a recent utility bill).
2. Ascertaining and verifying (if appropriate) the identity of the beneficial owners of a business.
3. Details on the purpose and intended nature of the business relationship i.e. knowing what you are going to do with/for them and why.

In addition to a check on customers, the University must also undertake due diligence on transactions including:

- Identifying and verifying the identity of a payer or payee, typically a student or donor
- Where the payment is to come from or be made by a third party on behalf of the student/customer, identifying and verifying the identity of that third party through letters or documents proving name, address and relationship to the student
- Where an organisation is not known to the University:
  - Look for appropriate formal documentation, and/or
  - Check websites, and/or
  - Request credit checks, and/or
  - Aim to meet or contact key sponsors as appropriate to verify validity of contact.
- Identifying and verifying the source of funds (i.e. where the funds in question are received from, for example, a bank account) from which any payment to the University will be made; and
- In some circumstances identifying and verifying the source of wealth (i.e. how the person that is making the payment came to have the funds in question, for example savings from employment) from which the funds are derived.

Both customer and geographical risk factors need to be considered in deciding the level of due diligence to be undertaken. Simplified customer due diligence is appropriate where the University determines that the business relationship or transaction presents a low risk of money laundering or terrorist financing, taking into account the risk assessment. Under MLR 2017, enhanced due diligence (EDD) is mandated for any business relationship with a person established in a high-risk third country. The list of high-risk countries as determined by the UK can be found here - High Risk Third Countries.

The UK government publishes frequently updated guidance on financial sanctions targets, which includes a list of all targets. This list can be found here - Financial Sanctions Targets.

The list provides information to assist in deciding whether the University is dealing with someone who is subject to sanctions. **The University will look to ensure that it has no relationship with any individuals on this list.**

A Politically Exposed Person (PEP) is someone who is or has been entrusted with a prominent public function within the last 12 months. Through their influence, many PEPs are in positions that could potentially be abused for committing money laundering. Under MLR 2017, organisations are required to have appropriate risk management systems and procedures in place to determine whether a customer or the beneficial owner of a customer, is a PEP. The University needs to be mindful of PEPs when developing relationships with new collaborative venture partners, potential donors and research partners. Appropriate compliance reports and risk screening for new partners will be used to mitigate the risk of working with PEPs.

12 Other Actions Taken

In addition to CDD, in order to minimise the potential for money laundering activities the University has the following procedures in place:

- Cash payments

The University does not accept cash payments for accommodation or tuition fees, or for any goods or services. Electronic payments are required for such payments.

- Requests for refunds

Precautions should also be taken in respect of refunds requested following a payment by credit card or bank transfer. In these cases, refunds must only be made by the same method to the same account. In the event of an attempted payment by credit or debit card being rejected, the reason should be checked prior to

accepting an alternative card.

Fees paid in advance by overseas students who have subsequently been refused a visa are only refundable where appropriate documentary evidence is provided to demonstrate the circumstances. Refunds should only be made to the person making the original payment, other than in very exceptional circumstances where this is not possible.

13 The Money Laundering Reporting Officer (MLRO)

The role of the MLRO is to be aware of any suspicious activity in the University which might be linked to money laundering or terrorist financing, and if necessary, to report it. They are specifically responsible for:

- Receiving reports of suspicious activity and maintaining a register of all reports of money laundering;
- Considering all reports and evaluating whether there is, or seems to be, any evidence of money laundering or terrorist financing;
- Reporting of all reports received, whether potential or actual cases of money laundering to the University Compliance Officer (UCO). As required, the UCO shall convene a meeting of the Fraud Response Group (FRG) in accordance with the University's Fraud Policy;
- Reporting any suspicious activity or transaction(s) to the NCA by completing and submitting a SAR;
- Following submission of a SAR, asking the NCA for consent (via a DAML SAR) to continue with any transactions that have been reported and ensuring that no transactions are continued illegally.

The MLRO for the University is the Chief Financial Officer:

- E-mail: mlro-reporting@strath.ac.uk

In their absence, the Director of Finance) will act as MLRO:

- E-mail:mlro-reporting@strath.ac.uk

14 Obligations and Disclosure Procedure to be followed by Associated Individuals

General expectations of associated individuals include:

- Discharge of duties in accordance with any contractual obligations and with due regard to University policies and procedures;
- Avoid handling money, goods or other items known or suspected to be associated with money laundering, or becoming involved with any services known or suspected to be associated with money laundering;
- Remaining vigilant and reporting any concerns related to suspected money laundering activity;
- Fully cooperating with any investigations into reported concerns;
- Maintaining confidentiality about any suspected or actual incidents involving the University.

Where associated individuals know or suspect that money laundering activity is taking or has taken place or become concerned that their involvement in a transaction may amount to a breach of the Money Laundering Framework, they must **disclose** this immediately to their line manager.

If associated individuals feel unable to discuss with their line manager, then direct contact should be

made with the MLRO.

If, in consultation with the relevant line manager, reasonable suspicion is confirmed, a disclosure report must be made to the MLRO. This disclosure should be made on the Proforma report attached in Appendix 3, as soon as practicable, by email, and giving as much detail as possible.

Following such a report to the MLRO, the relevant associated individual must not make any further enquiries into the situation unless instructed to do so by the MLRO. **At no time and under no circumstances should** the relevant associated individual **voice any suspicions to the person(s) suspected of money laundering to avoidthe offence of "tipping off" those who may be involved.**

Failure to disclose a suspicion of a case of money laundering is a serious offence and may result in disciplinary procedures being instigated and/or prosecution of the individual concerned.

15 Action and Disclosure by the MLRO

On receipt of a disclosure report, the MLRO will complete the response form, attached in Appendix 4. Consideration will be given to all relevant information, including:

- reviewing other relevant transaction patterns and volumes, and the length of any business relationship involved;
- reviewing the number of any one-off transactions, linked one-off transactions, and any identification evidence held.

The MLRO will advise the individual who submitted the disclosure when a response can be expected.

The MLRO will make other reasonable enquiries as appropriate in order to ensure that all available information is considered when deciding whether a report to the NCA is required. Enquiries will be made in such a way as to avoid any risk of "tipping off" those involved.

If the MLRO suspects money laundering or terrorist financing, they will suspend the transaction and make a Suspicious Activity Report (SAR) to the NCA in a timely manner.
However, a judgment will be made regarding how safe and practical it is to suspend the transaction without "tipping off" the suspect. It may be necessary to make the report as soon as possible after the transaction is completed.

Where the MLRO concludes that there are no reasonable grounds to suspect money laundering then consent will be given for transactions to proceed and the disclosure report will be marked accordingly.

The MLRO will keep a separate Register of Money Laundering report forms and will update this Register with any relevant documents as back up for the reasons for the decision, including a copy of any SARs made to NCA and other NCA correspondence.

Information that an authorised disclosure has been made should never be kept on the file relating to the person concerned.

16 Record-Keeping Requirements

By keeping comprehensive records, the University will be able to show that it has complied with the Money Laundering Framework and managed the money laundering risk. The University retains records for at least five years, or in line with the University Record Management Policy, after ceasing to transact with a customer including records of customer risk assessment, customer identity and verification and customer ongoing monitoring.

17 Training

In line with the Money Laundering Framework, all relevant individuals will receive training on this Policy and the wider aspects of money laundering. This will include new members of staff, where the training will first be completed as part of their induction. Record keeping is crucial to an effective training regime and a

record (or computer-based equivalent) should be kept verifying that such individuals have been trained on money laundering.

The frequency of training should be determined on a risk-based approach, but the periodicity should not exceed two years.

The University also subscribes to the training available from the British Universities Finance Directors Group website (BUFDG) and encourages staff to use this resource as much as possible. The anti-money laundering training module on BUFDG is mandatory for all Finance staff to undertake, due to the nature of their roles.

Appendix 1 – Legislation and Offences

Anti-money laundering laws that regulate financial systems, link money laundering (the source of funds) with terrorism financing (the destination of funds). The key elements of the UK anti-money laundering legislative and compliance framework that apply to universities include:

- Proceeds of Crime Act (2002)
- Terrorism Act (2000)
- Counter Terrorism Act (2008)
- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017)
- Anti Terrorism, Crime & Security Act (2001)
- Terrorism Asset Freezing Act (2010)
- Companies Act (2006)
- Criminal Finances Act (2017)
- Sanctions Act (2018)

The law concerning money laundering is complex and is increasingly actively enforced. It can be broken down into three main types of offences:

- the principal money laundering offences under the POCA;
- the prejudicing investigations offence under POCA; and
- offences of failing to meet the standards required of certain regulated businesses, including offences of failing to disclose suspicions of money laundering and failing to comply with the administrative requirements of the MLR 2017.

Appendix 2 – Risk Areas and Money Laundering Warnings Signs

Risk areas	
Jurisdiction Risk	Risks associated with transacting with certain locations and jurisdictions including, but not limited to, the University's countries of operation, the location of customers, suppliers and/or agents, and transactional sources/destinations.

Customer/3rd party Risk	Risks associated with the people and/or organisations that we undertake business with, including customers/3rd parties, beneficial owners, agents, contractors, vendors and suppliers. PEPs and Sanctioned Parties are also considered within this risk. Many of the University's customers are resident in the UK or EEA countries however some will come from/study overseas in potentially higher risk locations. The University also partners with overseas organisations for teaching and research purposes.
Distribution Risk	Risks associated with how the University undertakes business, particularly off campus, including direct and indirect relationships (via an agent or 3rd party), face-to-face, online and over the phone
Product/Service Risk	Risks associated with our standard product and service offerings. Whilst many of the University's operations do not present an opportunity for money laundering, there are risks around acceptance and processing of refunds.

The University assesses risks relevant to its operations and puts in place the processes and procedures deemed necessary to mitigate these risks. The University determines the appropriate level of due diligence by looking at the geographic and customer risk factors based on the EU Directive and set out in MLR 2017 and analysing the University's potential exposure to money laundering (the source of funds) or terrorist financing (the destination of funds).

Money Laundering Warning Signs or Red Flags

Payments or prospective payments made to or asked of the University can generate a suspicion of money laundering for a number of different reasons. Whilst it is not possible to give a definitive list of ways to spot money laundering, the following are examples of risk factors which may alone or collectively suggest the possibility of money laundering activity:

- payments or prospective payments from third parties, particularly where:
  - there is no logical connection between the third party and the student, or
  - the third party is not otherwise known to the University, or
  - a debt to the University is settled by various third parties making a string of small payments;
- payments from third parties who are foreign public officials or who are PEPs.
- payments made in an unusual or complex way;
- 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;
- donations which are conditional on particular individuals or organisations, who are unfamiliar to the University, being engaged to carry out work;
- requests for refunds of advance payments, particularly where the University is asked to make the refund payment to someone other than the original payer;
- a series of small payments made from various credit cards with no apparent connection to the student and sometimes followed by chargeback demands;
- 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;
- prospective payers are obstructive, evasive or secretive when asked about their identity or the source of their funds;
- prospective payments from a high-risk jurisdiction;
- the payer's ability to finance the payments required is not immediately apparent or the funding arrangements are otherwise unusual.

Appendix 3- Suspected Money Laundering - Report to the MLRO

CONFIDENTIAL – SUSPICIOUS ACTIVITY REPORT (SAR)
From:
Department:
Position within Department:
Contact Details (email /phone number):
DETAILS OF SUSPICIOUS ACTIVITY
Name(s) and address(es)/contact details of person(s) involved, including relationship with the University:
Description, value and timing of activity involved:
Nature of suspicions regarding activity (including details of any suspicious funds currently held by the University):
Details of any enquiries you may have undertaken to date:
Have you discussed your suspicions with anyone? If YES please provide details below:
Is any aspect of the transaction(s) outstanding and requiring consent to progress?
Any other relevant information that may be useful:
Signed:
Date:

Please return this form to electronically to mlro-reporting@strath.ac.uk or in person in an envelope marked private and confidential addressed to MLRO, Finance Directorate, Learning and Teaching Building, 49 Richmond Street, G1 1XU).

Appendix 4 - MLRO REPORT (to be completed by the MLRO)

MLRO REPORT (to be completed by MLRO only)
Date report received:
Date receipt of report acknowledged:
Consideration of Disclosure:
Action plan:
Outcome of consideration of Disclosure:
Are there reasonable grounds for suspecting money laundering activity? YES/NO
Does the matter need to be reported to the National Crime Agency (NCA)? YES/NO
If YES record the date reported to NCA
Is consent required from the NCA to proceed with a potentially suspicious transaction? YES/NO
If YES please confirm full details below:
If SAR is not reportable to NCA, please set out below the reason for nondisclosure:
Signed:
Date:

Appendix 5 - DEFINITIONS

Money Laundering Framework	The set of laws, rules, and regulations introduced to counter money laundering activities and terrorist financing. The key elements of the UK anti-money laundering legislative and compliance framework that apply to universities are set out in Appendix 1.
Money laundering	Money laundering is the illegal process of disguising the proceeds from criminal activity so that they appear to have come from a legitimate source.
Associated Person	Associated individuals in the context of this Policy includes, but is not limited to all staff, students, applicants, agents, volunteers, lay members, subsidiary companies of the University and to third parties, including academic partners, undertaking business on behalf of the University and its subsidiary companies.
Money Laundering Reporting Officer (MLRO)	The person with ultimate responsibility for the University's compliance with the UK anti-money laundering legislation. The role of the MLRO is to act as the focal point for the oversight of all activity relating to anti-money laundering. The MLRO should be made aware of any suspicious activity in the University which might be linked to money laundering or terrorist financing, and if necessary, to report it.
National Crime Agency (NCA)	The National Crime Agency, also known as the NCA, is a crime-fighting law enforcement agency responsible for leading the UK's fight to cut serious and organised crime.
Suspicious Activity Report (SAR)	A report to the NCA where there are reasonable grounds to suspect money laundering.
Defence Against Money Laundering (DAML)	A Defence Against Money Laundering (DAML) can be requested from the NCA where a reporter has a suspicion that property they intend to deal with is in some way criminal and that by dealing with it they risk committing one of the principal money laundering offences under the Proceeds of Crime Act 2002 (POCA). The term DAML refers to 'appropriate consent' given by the NCA to a firm to carry out an activity that is otherwise prohibited by the principal money laundering offences under the POCA.