

Anti-Money Laundering Policy

POLICY SCHEDULE	
Policy title	Anti-Money Laundering Policy (AML)
Policy owner	Director of Finance
Policy lead contact	Head of Financial Services
Approving body	Audit Committee
Date of approval	19 July 2017
Version no.	1
Related Policies, Guidelines and Procedures	Financial Regulations Fraud Response Plan Guide to raising concerns (to update) Donations Policy Financial Administration of Gifts and Donations Policy (to update) Records Management Policy
Review interval	3 yearly, or on changes to relevant legislation or guidance
Further info contact	Head of Financial Services

1. Introduction

The University is committed to the highest standards of ethical conduct and integrity and to preventing and detecting any criminal activity, including money laundering, involved in transactions or activities which involve the University.

This Policy outlines how the University will manage money laundering risks and comply with its legal obligations, ensuring that the highest standards of due diligence are applied.

The Policy sets out the procedure to be followed if money laundering is suspected, and defines the responsibilities of those to whom it applies.

2. Definitions

2.1 Anti-Money Laundering Legislation

The statutory and regulatory framework surrounding money laundering is centred on the following:

- Proceeds of Crime Act 2002 (“POCA”)
- Money Laundering Regulations 2007
- Terrorism Act 2002

The Money Laundering Regulations 2007 apply to a limited list of specific industries which does not include Universities and other Higher Education institutions. However, the Regulations set a best practice standard for policy, practice and procedure which the University has decided to adopt in this Policy.

POCA applies to individuals as well as corporate entities without limitation.

2.2 Money Laundering means any involvement or interaction with the proceeds of crime. This can apply to cash, goods, services and property (including intellectual property rights).

The Money Laundering Regulations 2007 applies to *“Money Laundering means exchanging money or assets that were obtained criminally for money or other assets that are ‘clean’. The clean money or assets don’t have an obvious link with any criminal activity. Money laundering also includes money that’s used to fund terrorism, however it’s obtained.”*

2.3 Money Laundering Offences are defined in legislation as:

- Concealing, disguising, converting, transferring criminal property or removing it from the UK.
- Entering into or becoming concerned in an arrangement which you know or suspect facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person.
- Acquiring, using or possessing criminal property.

Associated offences include:

Due Diligence Offences

- Failure to apply customer due diligence.
- Failure to apply on-going monitoring of business relationship and customer due diligence.
- Failure to comply with timing on verification of clients and any beneficial owner.
- Failure to apply enhanced customer due diligence and monitoring where required.
- Failure to keep required records.
- Continuing with a business relationship where unable to apply customer due diligence.

Disclosure Offences

- Making a disclosure to a person, which is likely to prejudice a money laundering investigation (“tipping off”).
- Failing to disclose [...].
- Prejudicing an investigation being carried out by a relevant authority into suspected money laundering activity.

3. Scope

3.1 Who it applies to

This Policy applies to the University and all of its subsidiary undertakings (referred to collectively as “the University” in this Policy), unless the Board of Directors of a subsidiary undertaking resolves to adopt an alternative policy which has been approved by the University’s Audit Committee.

This Policy applies to ALL University staff and others engaged by the University including those not directly employed by the University but who have responsibility for the administration or management of University funds, for example visiting and honorary staff, contract staff and the employees of contractors and agents acting on behalf of the University.

Members of Council and co-opted members of Council Committees, Directors and Officers of subsidiary undertakings are also required to comply with this Policy.

Any individual could be committing an offence under anti-money laundering laws OR POCA if they suspect money laundering activity and/or if they become involved in some way and/or fail to take appropriate steps in relation to it.

3.2 Where it applies

This Policy applies to the University's activities in the UK and overseas.

3.3 What it applies to

This Policy applies to all transactions and may include those involving agents and third parties in respect of the supply or acquisition of goods or services and the receipt of donated money or assets including property and other assets. Transactions includes those in which money is exchanged in the form of cash, cheque, card or bank transfers.

POCA applies to all transactions without restriction. The Money Laundering Regulations 2007 are restricted in scope to cash transactions in excess of 10,000 Euros which converts approximately to a sterling equivalent of £8,500.

Transactions undertaken by the University which fall within the scope of this Policy include but are not limited to the payment of fees by a student or their sponsor, agreements and contracts with commercial organisations, grants with government and non-government organisations and agencies, gifts and donations from individuals, associations and bodies corporate.

3.4 Third parties

Under this Policy the details of third parties who make payments to the University must be checked for all transactions over £8,500.

The University's policy on Donations and Philanthropic Giving sets out requirements for due diligence in respect of donors and benefactors.

3.5 International Students

Particular rules apply to International students studying in the UK. The [University's?] Immigration Service must be notified if a student with a visa discontinues their study. These cases are dealt with by the University's Student Systems and Records Office in the case of taught students, and the University's Research Services Administration Office for research students, who are responsible for the administration of student withdrawal.

3.6 Cash payments

Cash is defined as bank notes, coin or travellers cheques in any currency.

Large cash payments may be indicative of money laundering or of other offences under POCA and other legislation. They also present a security risk to staff and to those who carry large sums of cash in order to pay sums due. It is therefore the University's policy not to accept cash payments above £500 for any purposes including the payment of accommodation or tuition fees.

3.7 Card Payments

If in any doubt about the identity of the person attempting to make a card payment, the transaction should not be accepted. In the event of an attempted payment by credit or debit card being rejected, the reason should be checked and understood to be reasonable prior to accepting payment using an alternative card.

3.8 Requests for refunds

Precautions should 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.

Fees paid in advance by an international student who has subsequently been refused a visa are only refundable providing appropriate documentary evidence is available to evidence the circumstances. Refunds must only be made to the person making the original payment using the same method of payment used for the original funds receipt.

Where an international student accepts an offer from or transfers to an alternative university any payment received in advance may be transferred direct to the alternative university once it has been confirmed that the student has a valid offer to attend that institution and the institution is confirmed to be one which is recognised and regulated by the Higher Education Funding Council for England or the Scottish Funding Council.

3.9 Transaction Examples

The following are examples of transactions which indicate that a money laundering offence in principle or an offence under POCA may be being perpetrated:

- Payment by a person or company of any substantial sum in cash, particularly if they fail to provide satisfactory evidence to confirm their identity and address.
- A student wishing to pay a large amount in cash, particularly where the cash is used notes or small denominations.
- A person or company doing business with the University which lacks satisfactory paperwork, e.g. invoices that exclude VAT, failure to quote a VAT number or invoices issued by a limited company that do not contain the company's registered office and number.
- A person or company attempting to engage in circular transactions, where a payment to the University is followed by an attempt to obtain a refund from the University. (This may occur where a student pays a significant sum in fees, and then withdraws and seeks a refund).
- Requests for payments or refunds after funds have been paid into the University's bank account by a third party, particularly if there is a request to return money to a different account or individual to the payer.
- Unusual or unexpected large payments being made into the University's accounts or overpayments for no apparent reason particularly when there is no obvious legitimate source for funds.

- A secretive person or business e.g. one that refuses to provide requested information without a reasonable explanation.
- Involvement in a transaction of an unconnected third party without a logical reason or explanation.
- The payment of funds to the University which are then required to be transferred to another person or organisation without a legitimate University business reason. This may involve transfer of funds within the UK or cross border transfers.
- Significant changes in the size, nature, frequency of transactions with a customer that is without reasonable explanation.
- Cancellation, reversal or requests for refunds of earlier transactions. Repeated rejection of card payments and the use of multiple cards

Please note these examples are not intended to be exhaustive, but provide a general indication of the range of matters covered by this Policy.

4. What the University will do

The University undertakes to voluntarily adopt the requirements of The Money Laundering Regulations 2007 which represent a best practice standard for non-regulated organisations such as the University.

Requirement	Response
4.1 Appoint a Money Laundering Reporting Officer (MLRO) to receive, consider and report as appropriate, disclosure of suspicious activity reported by employees.	The University has appointed the Director of Finance as the MLRO. Day to day responsibility is delegated to Deputy Director of Finance and the Head of Financial Services.
4.2 Implement procedures to enable the identification and reporting of suspicious activity, such as complex or unusually large transactions, or unusual patterns of transactions which have no apparent economic or visible lawful purpose.	The MLRO will implement and maintain anti-money laundering procedures setting out that he/she will : <ul style="list-style-type: none"> • receive reports of suspicious activity from any member of staff, other person connected with the University, member of Council or co-opted member of a Council committee in the business; • respond to reports of suspected money laundering activity; • consider all reports and evaluate whether there is - or seems to be - any evidence of money laundering or terrorist financing; • Report any instances of money laundering or offences under POCA to the police.
4.3 Maintain procedures for customer identification in relevant circumstances.	It is important that controls are in place to identify the student, customer or other party dealing with the University: <ul style="list-style-type: none"> • In the case of students, this is done during enrolment checks by Student and Academic

	<p>Services, and checking identity against a valid University ID card is considered adequate evidence of identity for making payments to the University.</p> <ul style="list-style-type: none"> • Where a payment is made on behalf of a student, satisfactory evidence of the payer’s identity and relationship to the student concerned must be obtained. • If a person or an organisation is not known to the University, staff should look for satisfactory evidence of identity and this may include (but is not limited to) checking letter headed documents and web sites, requesting credit checks, or aiming to meet or contact key sponsors as appropriate to verify validity of contact. • Cheques drawn on an unexpected or unusual source should always be verified with regard to the validity of the source. • Cash payments in excess of £500 to any single account will not be accepted by the University. Any individual wishing to pay their tuition fee or other invoice in cash amounting to more than £500 will be declined and the person requested to pay using an alternative method i.e. bank transfer or card payment.
<p>4.4 Maintain adequate records of transactions</p>	<p>The MLRO will maintain a Register of all Report Forms.</p> <p>All disclosure reports and relevant documents will be retained in a confidential file for a minimum of six years.</p> <p>Student and Academic Services (Student identification), Development and Alumni Relations Office (donors) and Finance (all other customer identification evidence) must retain records of Student/Customer/Donor identification evidence for at least six years, as well as details of financial transactions carried out.</p>
<p>4.5 Additional steps In addition, the University will implement effective policies and controls to prevent and detect illegal activity.</p>	<p>This will be achieved through the following:</p> <ul style="list-style-type: none"> • Reporting any instances of suspected money laundering or associated offences under POCA to the University’s Audit Committee. • Create and annually review Anti-Money Laundering Policy for approval by the University’s Audit Committee • Perform regular risk assessments of activities to

	<p>identify areas of operation most vulnerable to money laundering and offences under POCA;</p> <ul style="list-style-type: none"> • Regularly review and revise internal controls in light of the outcomes of risk assessment and vulnerable business activities. • Undertaking appropriate staff awareness and training
--	---

5. What the University expects staff and other persons who come under this Policy to do

5.1 Anti Money Laundering training

The University will ensure that new members of the Finance Division receive appropriate anti-money laundering training as part of their induction. Each member of the team will be required to sign a record to verify that they have read and understood this AML Policy. Refresher training will take place at each revision of the Policy, at which point all staff will be asked to update their signed record.

This Policy will be drawn to the attention of senior University managers who will be responsible for identifying staff in their areas with responsibilities for, or potential exposure to, relevant activities such as student checks at enrolment or financial transactions. These staff will be subject to the same anti money laundering training requirements as the Finance Division.

5.2 Handling the proceeds of crime

All staff and other persons engaged by the University must avoid handling any money, goods or other items known or suspected to be associated with the proceeds of crime, or becoming involved with any services known or suspected to be associated with the proceeds of crime.

5.3 Reporting requirement

Anyone who suspects that money laundering activity or an offence under POCA is taking or has taken place, or who becomes concerned about their involvement in a transaction or series of transactions must disclose their suspicions and concerns as soon as possible to the MLRO.

Identification and reporting may arise from several different means including:

- The University Financial Regulations requirement (section 2.3) that members of staff, students or members of Council suspecting fraud or financial irregularity in the University should report it as soon as possible to the Director of Finance or the University Chief Operating Officer;
- The University’s procedure on raising concerns (‘whistleblowing’ policy);
- The operation of effective systems of internal control, including clear objectives, segregation of duties and proper authorisation procedures; and
- The work of the internal auditors, in reviewing the adequacy and effectiveness of the internal control systems.

Where suspicion of fraud or financial irregularity is captured through any route, including those set out above, it should be reported as soon as possible to the MLRO (Director of Finance).

If any suspected fraud or financial irregularity relates personally to the Director of Finance, or the

Director of Finance is unavailable, members of staff, students or members of Council should refer the matter to the University Chief Operating Officer.

If the suspected fraud or financial irregularity relates personally to the Director of Finance and the University Chief Operating Officer, members of staff, students or members of Council should refer the matter to the Vice Chancellor or the Deputy Vice Chancellor.

5.4 Cooperating with investigations

Any individual who reports suspicions or concerns under paragraph 5.3 of this Policy must co-operate fully with any investigation into reported concerns. They must maintain confidentiality about any suspected or actual incidents involving the University and must not undertake enquiries into the situation or discuss their concerns with anyone else at any time, unless instructed to do so by the MLRO. This is to avoid “tipping off” those who may be involved, which may be an offence under the relevant regulations and legislation in itself.

Failure to report money laundering concerns or "tipping off" anyone who may be involved in the money laundering activity may result in a referral being made to HR to consider whether further action should be taken, including under the University's disciplinary procedures.

6. How to report a concern

Any person suspecting money laundering activity or an offence under POCA or becomes concerned about their involvement in a transaction or series of transactions should:

- use the Money Laundering Report Form at the end of this Policy to report the concern, giving as much information as possible, in writing, and without delay;
- send the Report Form as soon as possible to the MLRO marking the email or envelope “Confidential”;
- Remember not to make further enquiries into the situation or discuss their concerns with anyone else at any time, unless instructed by the MLRO. This is to avoid committing the offence of “tipping off” those who may be involved.

7. What the University will do in response to concerns reported to it

7.1 MLRO response

Upon receipt of a completed Money Laundering Report Form, the MLRO will complete the Response Form. 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;
- advising the reporter of the timescale within which a response can be expected.

7.2 MLRO inquiries

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

7.3 Reporting

If the MLRO concludes that money laundering or an offence under POCA may be being or may have been perpetrated he/she will normally suspend the transaction and report the matter to the police immediately. 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 report the matter as soon as possible without suspending the transaction.

The MLRO will report all formally reported suspicions of suspected money laundering and/or offences under POCA to the University’s Audit Committee whether or not it has been decided to report the matter to the police.

7.4 Maintaining a register

The MLRO will keep a separate Register of money laundering Report Forms and will update this Register with any relevant documents, including a copy of any reports and correspondence exchanged with the police. Reports and associated documentation should be kept for six years.

7.6 Reporting to the Funding Council

The MLRO should have regard to Funding Council’s guidance on the reporting of “serious incidents” in order to establish whether suspected or actual money laundering should be reported to them. Specifically, donations over £25,000 from unknown donors, or where the source cannot be verified, must be reported as a “serious incident”.

8.0 Disciplinary and other procedures

Any member of staff or other person engaged by the University (as referred to in section 3) who has failed to follow the University’s Anti Money Laundering Policy or any instructions given separately by the MLRO, will be referred to Human Resources and consideration will be given as to whether further action is necessary or warranted under the University’s procedures (including the disciplinary procedure) or under the terms of the individual or organisation’s relationship with the University.

This may include, but is not limited to the following:

- a. The University may decide to follow its disciplinary procedure against an employee, which could result in dismissal.
- b. Any member of Council or co-opted member of a Council committee may be removed under regulation 5 COUNCIL: 21. Removal of members of Council.
- c. Any other person or organisation may be subject to the termination of their relationship with the University, in accordance with any provisions, which govern that relationship.

[Appendix 1 : Suspected Money Laundering Reporting Form]

CONFIDENTIAL - Suspected Money Laundering Reporting Form <i>Please complete and send this to the Money Laundering Reporting Officer ("MLRO") using the details below and append any supporting documents</i>	
From:	School/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:
<i>Please do not discuss the content of this report with anyone, particularly those you believe to be involved in the suspected money laundering activity described. To do so may alert or tip off those involved, which may be an offence under anti-money laundering legislation and require reporting to the police. The University may also decide to refer any such actions to Human Resources for consideration as to whether further action is required.</i>	

This form should be scanned and sent as a pdf file to the MLRO.