Anti-Money Laundering Policy			**Ref: VC0004**
Brief Description & Purpose:	This Policy outlines how the University and its employees will manage money laundering risks and comply with its legal obligations under the Proceeds of Crime Act 2002, the Terrorism Act 2002 and the Money Laundering Regulations 2007		
Applicable to (list cohorts):	**Staff:** All staff and governors	**Students:** Not applicable	**Third Parties:** Not applicable
Effective From:	21st May 2012	**Last Review Date:**	10th October 2022 (format and nomenclature changes)
Approval Authority:	Board of Governors	**Approved:**	21st May 2012
Executive Owner:	Georgina Bailes/ Simon Newitt	**Business Owner:**	Tina Hannant/ Jack Taylor
Next review date	August 2025	**Publication External Y/N**	Y

1. Introduction

Current legislation applies a broad definition of money laundering activities and the range of activities where the legislation can apply. Historically, the primary focus was on banks and the financial sector but all companies and institutions, including universities, are now subject to the legislation. The University is committed to high standards of ethical behaviour and preventing and detecting all criminal activity, including money laundering. It is no longer acceptable to conduct business on trust alone.

Money laundering regulations apply to cash transactions in excess of 15,000 Euros (approximately £13,000). However, POCA applies to all transactions and can include dealings with agents, third parties, property or equipment, cheques, cash, or bank transfers.

Although instances of suspected money laundering are likely to be rare, given the nature of services provided by the University, failure to comply with legal requirements could have significant implications for both the University and individuals concerned. There are specific requirements around the reporting and investigation of concerns around money laundering.

2. Policy Detail

2.1 The University's approach to fraud, bribery, and corruption

- The University will seek to prevent and detect money laundering by a variety of measures including: risk assessments to identify University activities and areas of operation most vulnerable to money laundering;
- staff awareness and training
- appropriate due diligence checks, applied in relation to 'know your customer' principles;
- strong internal controls, to prevent and detect such activity;
- learning from incidents by improving internal controls.

2.2 Expectations of University staff

General expectations of university staff include:

- To discharge their duties in accordance with their contractual obligations and with due regard to University policies and procedures;
- To undertake all training associated with this Policy;
- To 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.
- To remain vigilant and report concerns related to suspected money laundering activity.
- To co-operate fully with any investigations into reported concerns.
- To maintain confidentiality about any suspected or actual incidents involving the University.

3.1 **Disciplinary Routes Where Breach in Policy Occurs**

3.1.1 The University will not tolerate money laundering activity, carried out by its own staff or by third parties involved with the University's activities.

3.1.2 The University will encourage its staff, contractors, and related parties to report concerns and suspicious activity. (See "reporting concerns").

3.1.3 Staff are reminded that money laundering legislation applies to ALL employees. Staff could be committing an offence if they suspect money laundering (or if they become involved in some way) and do nothing about it. Examples of warning signs and "red flags" are shown at Appendix A.

3.1.4 If a member of staff suspects that money laundering activity is or has taken place or if any person becomes concerned about their involvement then staff should follow the reporting process outlined below. Once reported, staff should not 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.

3.1.5 The University has identified staff to whom concerns should be reported and who will refer concerns to the Serious Organised Crime Agency ("SOCA") if required.

Failure to report money laundering concerns or "tipping off" anyone who may be involved in the situation may result in the member of staff being personally liable to prosecution under the 2007 Regulations.

3.1.6 Money laundering legislation requires concerns to be reported as outlined below. All actual or suspected instances of irregularity relating to the scope of this Policy should be reported in writing without delay- see flowchart of the reporting channels for raising concerns.

3.1.7 If a person suspects money laundering activity or becomes concerned about their involvement then they should:

- use the Money Laundering Report Form concern as detailed in the attached procedure, giving as much information as possible;
- send the Report Form as soon as possible to the Finance Director, who acts as the University's Money Laundering Reporting Officer ("MLRO"). **Please mark the envelope "confidential".**

Important: Avoiding the criminal offence of "tipping off"

3.1.8 Once reported, staff should make no further enquiries into the situation or discuss their concerns **with anyone else at any time**, unless instructed by the MLRO. Neither should they make

any reference on a file to a report having been made. The appropriate records will be kept in a confidential manner in by the MLRO. Following this advice will protect employees from committing the criminal offence of "tipping off".

3.2 How the University will respond to concerns

3.2.1 Consideration of suspected Money Laundering

3.2.2 Upon receipt of a completed Money Laundering Report Form (Part 1), the MLRO must complete Part 2 of the form. Consideration will be given to all relevant information, including:

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

The person making the report will be advised of the timescale within which a response can be expected.

3.2.3 The MLRO will make other reasonable inquiries as appropriate in order to ensure that all available information is considered when deciding whether a report to the SOCA is required. Inquiries will be made in such a way as to avoid any appearance of tipping off those involved.

3.2.4 If the MLRO suspects money laundering or terrorist financing they will normally suspend the transaction and make a Suspicious Activity Report to SOCA. However, a judgment should 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.

3.3 Human Resources considerations

3.3.1 Disciplinary action

3.3.2 The University may follow disciplinary procedures against any member of staff who has committed a money laundering offence, which could result in dismissal.

3.3.3 References for employees disciplined or prosecuted for money laundering

3.3.3.1 References for employees disciplined or prosecuted for money laundering Any request for a reference for a member of staff who has been disciplined or prosecuted for money laundering shall in all cases be referred to the Director of Human Resources, who will respond having regard to employment law.

4. Roles and Responsibilities

Role	Responsibility
Chief Financial Officer	• Nominated Money laundering Reporting Officer (MLRO) • Implementing and maintaining anti-money laundering procedures and responding to reports of suspected money laundering activity.
Deputy Chief Financial Officer	• MLRO in absence of the Finance Director
MLRO	• Receiving reports of suspicious activity from any employee in the

	business and maintaining a Register of all Report Forms. • Considering all reports and evaluating whether there is - or seems to be - any evidence of money laundering or terrorist financing. • Reporting any suspicious activity or transaction to the SOCA by completing and submitting a Suspicious Activity Report. • Asking SOCA for consent to continue with any transactions that they have reported and making sure that no transactions are continued illegally. • keep a separate Register of money laundering Report Forms and will update this Register with any relevant documents, including a copy of any "Suspicious Activity Reports" made to SOCA and other SOCA correspondence. Current SOCA guidance requires that Report Forms and associated documentation should be kept for at least five years.

5. Definitions

Money Laundering- any involvement or interaction with the proceeds of crime. This can apply to cash, goods, services, and property (including intellectual property rights). The statutory framework surrounding money laundering is centred on the following legislation:

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

This legislation now defines the following money laundering offences :

- 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.

Due Diligence

- 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.

Disclosures

- Making a disclosure to a person which is likely to prejudice a money laundering investigation ("tipping off").
- Failing to disclose.
- Prejudicing an investigation.

6. Related Policies, Procedures and Other Resources

- Public Interest Disclosure "Whistleblowing" Policy
- Staff Code of Conduct
- Disciplinary Procedure

7. Version

Version No.	Reviewer	Date	Changes
1.0	Chris Reilly & Susan O'Donnell	26th November 2012	Revised role titles
1.1	Richard Elliott	10th October 2022	Policy format change, links added, nomenclature and role updates

Appendix:

A. **Examples and "Red Flags"**

Associated Procedure & Guidance Notes (for MLRO use only)

External Reporting procedure (for SOCA notification)

The examples below are not intended to be exhaustive but provide a general indication of the range of matters covered by this Policy.

Money laundering: Examples of suspicious activity
Payment by a person or company of any substantial sum in cash (over £10,000), particularly if they fail to provide proper evidence to confirm their identity and address.
A person or company doing business with the University lacks proper paperwork, e.g. invoices that exclude VAT, failure to quote a VAT number or invoices issued by a limited company that lack the company's registered office and number.
A person or company attempts to engage in circular transactions, where a payment to the University is followed by an attempt to obtain a refund from the University's accounts. (This may occur where a student pays a significant sum in fees, and then withdraws and seeks a refund).
Unusual or unexpected large payments are made into the University's accounts.
A secretive person or business e.g. that refuses to provide requested information without a reasonable explanation
Students requesting a large cash transaction, particularly where the cash is used notes or small denominations.
Absence of any legitimate source for funds received
Overpayments for no apparent reason.
Involvement of an unconnected third party without a logical reason or explanation. Significant changes in the size, nature, frequency of transactions with a customer that is without reasonable explanation.
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
Cancellation, reversal or requests for refunds of earlier transactions