ANTI-MONEY LAUNDERING AND COUNTER TERRORIST FINANCING POLICY

Version Number 4.0

Effective from June 2024

Author: Head of Financial Accounting

Document Control Information

Revision History incl. Authorisation:

Author	Summary of changes	Version	Authorised & Date
Ian Dempsey	*Formalises an existing internal policy that has been written using the BUFDG template.*	1	Approved at ARC 11th June 2020
Ian Dempsey	*Highlight that this applies to subsidiary companies*	2	Highlighted by ARC September 2020
Ian Dempsey	*Clarification of 3 main types of offence – Section 3 Scope, expanded the section on possible signs of money laundering – Section 4 and risk mitigations introduced at Salford – Sections 6 & 7.*	3	ARC June 2022
Carla Elliott	*Inclusion of: Terrorist Financing within policy, Introduction for clarity for all staff and a due diligence section as well as rearranging order so easier to understand.*	4	To be reviewed June 2024

Policy Management and Responsibilities:

Owner	This policy is issued by the Deputy Chief Executive and Chief Finance Officer who has the authority to issue and communicate policy on financial matters of the University. The Deputy Chief Executive and Chief Finance Officer has delegated day to day management and communication of the policy to the Payment Security Compliance Manager within the Income and Treasury Team. All subjects of the Policy will be responsible for engaging with and adhering to this policy.
Others with responsibilities (please specify):	

Author to complete formal assessment with the following advisory teams:

Equality Analysis (E&D, HR)	1. This is mandatory. Specify date completed and brief outcome. Email the completed EIA to equity@salford.ac.uk
Legal implications (LPG)	N/A
Information Governance (LPG)	N/A
Student facing procedures (QEO)	N/A
UKVI Compliance (Student Admin)	N/A

Review:

Review due:	Bi-Annually with report back to ARC every two years by July 2026
Document location:	https://www.salford.ac.uk/governance-and-management/finance-policies

Document dissemination and communications plan: Mandatory online courses for all new starters (see 1.2) and then staff (see 1.2) to repeat every 2 years.

The owner and author are responsible for publicising this policy document.

1.0 Introduction

1.1 What is this document?

This document explains the steps the University and its subsidiaries are taking to prevent and deter money laundering and terrorist financing. It details the responsibilities of all persons associated with the University and its subsidiaries in preventing and deterring these criminal activities.
It details the appropriate action that should be taken when money laundering or terrorist finance is suspected or detected.

1.2 Who is it for?

- **All staff**, but particularly those who are involved in the decision to accept students or bidding and invoicing for research and enterprise activity, on behalf of the University and its subsidiaries.
- Staff who are involved in identifying whether students come from sanctioned countries and other higher risk customer categories.
- Staff who are involved with the processing of income receipts or refunds.

1.3 Who can you contact regarding this document.

The Anti Money Laundering nominated Officer (Director of Finance) or the Payment Security Compliance Officer within the Income and Treasury Team (see 10.3).

1.4 Background:

Universities and their students have in recent years seen an increase in targeting by criminals who are seeking out new ways to commit money laundering and fraud offences.

Examples include students being targeted by credit card fraudsters, fake receipt scams and being used as Money Mules.

The University has taken steps to reduce these risks by introducing a designated Payment Security Compliance Officer and removing the options to pay by cash or over the counter at the university's day to day bankers - Lloyds bank.

1.5 Policy Aims

The University is committed to ensuring the highest standards of probity in all its financial dealings. 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 it. 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 policy sets out those obligations, the University's response, and the procedures to be followed to ensure compliance.

The University of Salford is committed to the highest standards of openness, transparency, and accountability and to conducting its affairs in accordance with the requirements of the relevant funding and regulatory bodies. The University of Salford has a zero-tolerance approach to money laundering and the policy applies to activity both at home and abroad and to any activity with university partners.

2.0 Scope

This policy applies to all members of the University including staff, students and to third parties, including agents and academic partners undertaking business on behalf of the University. Money laundering is a criminal offence and can incur a custodial sentence of up to fourteen years and an unlimited fine.

Offences include:

- Failing to report knowledge and or suspicion of money laundering.
- Failing to have adequate procedures to guard against money laundering.
- Knowingly assist in money laundering.
- Tipping-off suspected money launderers.
- Recklessly making a false or misleading statement in the context of money laundering

The University could also face a range of sanctions for non-compliance, therefore disciplinary action under the University's procedures may be taken against members of staff who fail to comply with this policy.

3.0 Definitions & Legislative Context

3.1 What is money laundering?

Money laundering is the process of taking profits from crime and corruption and transforming them into legitimate assets. It takes criminally derived 'dirty funds' and converts them into other assets so they can be reintroduced into legitimate commerce. This process conceals the true origin or ownership of the funds, and so 'cleans' them.

There are three main types of offences which apply to any property (e.g. cash, bank accounts, physical property, or assets). It is a crime to:

1. Conceal, disguise, convert or transfer criminal property or to remove it from the United Kingdom.
2. Enter an arrangement that you know, or suspect makes it easier for another person to acquire, retain, use, or control criminal property; and
3. Acquire, use, or possess criminal property provided that adequate consideration (i.e. proper market price) is not given for its acquisition, use or possession.

University staff can commit these offences when handling or dealing with payments to the University if they make or arrange to make a repayment, they risk committing the first two offences, and if they accept a payment, they risk committing the third offence.

There are three stages in money laundering: placement, layering and integration.

- Placement is where the proceeds of criminal activity enter the financial system.
- Layering distances the money from its illegal source through layers of financial transactions.
- Integration involves the re-introduction of the illegal proceeds into legitimate commerce by providing an apparently genuine explanation for the funds.

Examples of money laundering offences include tax evasion, theft, fraud, bribery, corruption, smuggling, modern slavery, human trafficking, drug trafficking and illegal arms sales.

3.2 What legislation applies?

The law concerning money laundering is complex. The Money Laundering, Terrorist Financing & Transfer of Funds Regulations 2017 (MLR 2017) came into force on 26 June 2017 which implement the EU's 4th Directive on Money Laundering and replace the Money Laundering Regulations (MLR 2007). The UK Anti-Money Laundering (AML) framework also incorporates the Proceeds of Crime Act 2002. MLR 2017 adopts a more risk-based approach towards anti – money laundering and how due diligence is conducted.

3.3 Defences to Money Laundering offences

Where the university suspects money laundering, it must immediately suspend activity on the payers account and submit a report to the relevant body. University staff could be committing an offence if they 'tip off' a person that a report has been made against.

3.4 Failure to Disclose Offence

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

3.5 The Offence of Prejudicing Investigations / Tipping-Off

The purpose of making an authorised disclosure to the National Crime Agency is to allow it 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 Proceeds of Crime Act 2002 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. University staff can commit this offence if they tell a person an authorised disclosure has been made in their case.

The University could also face a range of sanctions for non-compliance, imposed by HM Revenue and Customs (HMRC) and /or the Financial Conduct Authority (FCA).

Therefore, disciplinary action under University procedures may be taken against members of staff who fail to comply with this policy.

University staff could be committing an offence if they 'tip off' a person that a report has been made against.

4.0 Terrorist Financing

4.1 What is Terrorist Financing?

Whereas money laundering is concerned with the process of concealing the illegal origin of the proceeds from 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. Here, 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 re-imbursement, to be made to an account in a jurisdiction with links to terrorism.

4.2 What legislation applies?

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

i) raising, possessing, or using funds for terrorist purposes.

ii) becoming involved in an arrangement to make funds available for the purposes of terrorism; and

iii) 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.

It is an offence when a person believes or suspects Terrorist Finance and does not report it. 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.

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.

4.3 Defences to the Principal Terrorist Finance Offences:

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.

5.0 Transactional due diligence (Know Your Customer):

5.1 Transactions:

Due diligence is the process by which the University assures itself of the provenance of funds it receives and that it can be confident that it knows the people and organisations with whom it works. In this way the University is better able to identify and manage risk. Due diligence should be carried out before the funds are received. Funds must not be returned before due diligence has been reviewed.

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. To discharge the "reasonably satisfied" the University must obtain a minimum level of personal information from a customer.

5.2 This includes:

- Identifying and verifying the payer/payee identity, typically this will be a student payment.
- Identifying where the payment is to come from or to be made by a third party on behalf of the student, donor, or debtor.
- Identifying and verifying the identity of that third party. Letters or documents proving name, address and relationship should be obtained.
- Identifying and verifying the source of funds from which any payment to the university will be made.
- Identifying and in some circumstances verifying the source of wealth from which to funds are derived.

If an organisation is not known to the University, then Letter Headed documents, website and credit checks should be undertaken as appropriate. 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.

In most cases the University's exposure to money laundering is likely to be low. Financial due diligence is already considered as part of bidding for research, consultancy, and collaborative provision. However, in certain instances if the University is considering establishing a business relationship in a high-risk country or with a politically exposed person, then appropriate advice should be taken from the Money Laundering officer (MLRO) pre entering the arrangement.

5.3 Financial Sanctions
What are Financial Sanctions?

Financial sanctions are imposed by the Government and may apply to individuals, entities, and governments, who may be resident in the UK or abroad.

Financial sanctions orders prohibit a firm from carrying out transactions with a person or organisation (known as the target). In some cases, the order will prohibit a firm from providing any financial services to the target.

How do we know who is sanctioned?

The University's bankers advise of any high-risk countries where financial transactions are either prohibited or heavily restricted. The UK government publishes frequently updated guidance on financial sanctions targets, which includes a list of all targets. This guidance can be found at:
https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets

If the University is planning to admit any students or undertake any research or consultancy activities with entities and/or individuals in any of the following countries, please consult with either the MLRO or deputy so that the University can review the register and ensure that the proposed activity is not with a sanctioned individual or organisation:

- Afghanistan
- Belarus
- Bosnia and Herzegovina
- Burundi
- Central African Republic
- Democratic People's Republic of Korea

- Democratic republic of Congo
- Guinea
- Republic of Guinea-Bissau
- Haiti
- Iran
- Iraq
- Libya
- Mali
- Myanmar
- Nicaragua
- Russia
- Somalia
- South Sudan
- Sudan
- Syria
- Venezuela
- Yemen
- Zimbabwe

6.0 Risk Assessment

6.1 Transaction Risk Assessment

Having completed its due diligence exercise, the University will assess the money laundering and terrorist finance risk associated with the proposed transaction.

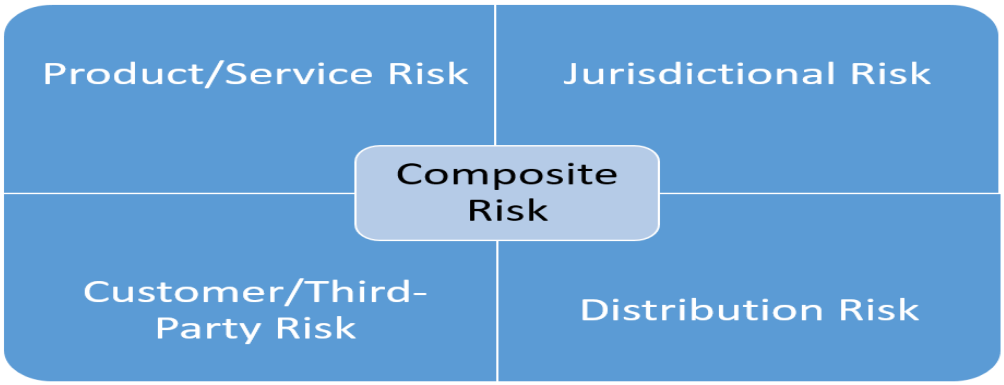
Due to the number of transactions processed by the University, the University has adopted a risk-based approach to manage this task. Using the risk scoring matrix found at **Appendix B,** a score will be calculated for each transaction and a decision made as to the risk of Anti Money Laundering or Terrorist Financing.

Where the transaction is considered suspicious **(see Appendix A)** or the member of staff dealing with the case otherwise considers there is a suspicion of money laundering or terrorist finance, they must report the case as soon as practicable to the Money Laundering Reporting Officer.

6.2 Areas to consider:

Money laundering regulation 2017 requires the university to undertake a risk assessment and assess its exposure to money laundering.

There are 4 main areas that need to be considered to assess its overall risk.



Product / Service Risk – This is the risk associated with delivery of university activity including teaching, research, enterprise, and conferencing activity.

Jurisdictional Risk – This is the risk associated with the Universities' countries of operation, location of students and customers, suppliers, and agents.

Customer/Third-Party Risk – This 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.

Distribution Risks – This 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.

Whilst much of the University of Salford's financial activity could be considered relatively low risk from the perspective of money laundering, all staff need to be vigilant against the financial crime and fraud risks that the university faces day-to-day.

6.4 Risk Mitigation

The university will:

- Conduct an appropriate risk assessment to identify and assess areas of risk money laundering and terrorist financing particular to the University.
- Implement controls proportionate to the risks identified.
- Establish and maintain procedures to conduct due diligence on funds received.
- Review policies and procedures annually and carry out on-going monitoring of compliance with them.
- Appoint a MLRO to be responsible for reporting any suspicious transactions to the relevant bodies.
- Provide training to all relevant members of staff, including temporary staff, on joining the University, and provide refresher training.
- Maintain and retain full records of work done pursuant to this policy.

The University has a number of policies and procedures in place to minimise the risk of money laundering – in particular the Financial Regulations which can be found at https://www.salford.ac.uk/governance-and-management/finance-policies

7.0 Unusual or Large payments

The University will investigate and establish what they are for. The University's bankers also advise on high-risk countries where financial transactions are either prohibited or heavily restricted. International students are encouraged to pay through flywire who carry out their own AML checks and therefore reduces the risk to the University.

8.0 Cash Thresholds

MLR 2017 has reduced the limit for eligible cash transactions from €15,000 [£13,000] to €10,000 [£8,800] and is extended to receiving, as well as making, payments in cash.

In the light of this and the security risk of carrying large amounts of cash, the University continues to no longer accept cash payments for tuition fees.

The University bank – Lloyds has also recently advised that on a best endeavours basis they will no longer be taking cash deposits over the counter without a pre-printed paying in slip. Again, this is to try and reduce the potential for money laundering.

9.0 Processing Refunds:

The University will undertake appropriate checks before processing any refunds and funds can only be refunded back to the original payer and cannot be refunded to a third party. Where the original payment has been received from abroad the refund will be to the foreign bank account and not to a UK bank account.

10.0 Roles and Responsibilities

10.1 Overall responsibility

The Deputy Chief Executive and Chief Finance Officer has responsibility for the Anti-Money Laundering Policy, which will be reviewed by the Audit and Risk Committee.

10.2 Money Laundering Reporting officer (MLRO)

The MLRO is the primary contact for any further information or to report any suspicious activity. The MLRO is:

Andrew Crozier
Director of Finance
Email**:** A.Crozier@salford.ac.uk

And the deputy is:

Ian Dempsey
Head of Financial Accounting
Telephone 0161 295 0180
Email: I.M.Dempsey@salford.ac.uk

The MLRO is responsible for:

- receiving reports of suspicious activity from any employee in the business.

- 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 Serious Organised Crime Agency (SOCA) by completing and submitting a Suspicious Activity Report.
- asking SOCA for consent to continue with any transactions that must be reported and making sure that no transactions are continued illegally.

10.3 Other contacts:

Payment Security Compliance Officer:

Carla Elliott
Telephone 0161 295 8198
Email: c.elliott8@salford.ac.uk

10.4 All members of the University – Reporting Suspicious Activity

A member of the University who needs to report suspicious activity must complete the Suspicious Activity Report (SAR) which is detailed in **Appendix E.** They 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. For further guidance see **Appendix C and Appendix D.**

Money laundering legislation applies to **all** member of the University. Members of the University could be committing an offence if they suspect money laundering (or if they become involved in some way) and do nothing about it. Potential Red flags are highlighted in Section **Appendix A.**

The MLRO will report any findings to the Deputy Chief Executive and Chief Finance Officer who will carry out any investigation in accordance with the Counter Fraud Policy and Response Plan.

10.5 Training

Finance will ensure that members of staff with financial responsibility receive appropriate money laundering training. Refresher training will take place at each revision of the policy.

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. The University will make and retain anti-money laundering training records for a period of 5 years.

11.0 Related Documentation

The following related documents can be found at:

https://www.salford.ac.uk/governance-and-management/finance-policies

- Financial Regulations
- Counter Fraud Policy
- Anti-Bribery Policy (and guidance)
- Criminal Finance Act Policy with links for other related policies below:

Register of Interests, Gifts and Hospitality Policy (Declaration and Management of Conflicts of Interest:

https://www.salford.ac.uk/governance-and-management

The Whistle Blowing Policy at:

https://www.salford.ac.uk/sites/default/files/2022-04/UOS-whistleBlowingPolicyV4.1.pdf

Disciplinary policy

https://testlivesalfordac.sharepoint.com/sites/HumanResources/Shared%20Documents/Forms/AllItems.aspx

12.0. Review, Approval and Publication

The Anti- Money Laundering Policy is subject to review every 2 years by the Deputy Chief Executive and Chief Financial Officer or following a change to relevant UK legislation.

Updates to the Anti- Money Laundering Policy will be reviewed by the Audit and Risk Committee and final approval will be given by University Council.

Appendices

Appendix A: Examples of suspicious activity

Appendix B: Payment Transaction Risk Scoring matrix

Appendix C: Guidance for staff

Appendix D: Guidance for line managers

Appendix E: Suspicious Activity Report

Appendix F: MRLO report

Appendix A: Examples of Suspicious Activity:

a) large, unexpected payments.

b) multiple small payments to meet a single payment obligation.

c) Payments or prospective payments from third parties, particularly where:

(i) there is no logical connection between the third party and the student, or

(ii) where the third party is not otherwise known to the University, or

(iii) where a debt to the University is settled by various third parties making a string of small payments.

d) Payments from third parties who are foreign public officials or who are politically exposed persons ("PEP").

e) Payments made in an unusual or complex way.

f) 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.

g) Donations which are conditional on individuals or organisations, who are unfamiliar to the University, being engaged to carry out work.

h) Requests for refunds of advance payments, particularly where the University is asked to make the refund payment to someone other than the original payer.

i) A series of small payments made from various credit cards with no apparent connection to the student and sometimes followed by chargeback demands.

j) 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.

k) Prospective payers are obstructive, evasive, or secretive when asked about their identity or the source of their funds or wealth.

l) Prospective payments from a potentially risky source or a high-risk jurisdiction.

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

n) A person or company undertaking business with the University fails to provide proper paperwork (examples include charging VAT but failing to quote a VAT

number or invoices purporting to come from a limited company, but lacking company registered office and number)

o) 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.”

This list is not exhaustive and money laundering can take many forms. If there are any concerns, then these should be raised with the Money laundering Reporting Officer

Appendix B: Payment Transaction Risk Scoring Matrix

Risk Score	Nationality / Domicile	Remitter Relationship	Payment Method	Number of payment attempts	Transaction Value
1	United Kingdom	Student	UK card/bank account	<3 - same payer details	
2		Parent/Guardian	Third party provider who does due diligence on payer		
3	EU			3-10 - same payer details	
4		Other 'Relative'	International card		
5					
6			Unknown third-party provider		
7	Law Society High Risk AML Countries PEP				
8	FATF Grey list		International bank transfer		
9	HMRC increased risk list	Unrelated			
10	FATF Blacklist, HMRC high risk list, countries with prevalent ITVS networks (China, India, Nigeria)	Unknown/ Suspicious and/or multiple payers		3+ - different payer details	

Range	Risk	Action Required
0-8	Low	No additional checks required, and payment may be allocated to account.
9-29	Medium	Further checks required to mitigate risks.
30-44	High	Further checks required to mitigate risks and Payment Security Compliance Officer sign off required.
45-55	Very High	Refer to Payment Security Compliance Officer as SAR and DAML likely required.

Appendix C: Guidance for Staff

Q. What should you do if you suspect money laundering?

• Do make an immediate note of your concerns. Make a note of all relevant details, such as what was said in telephone or other conversations, the date, time, and the names of any parties involved.

• Do convey your suspicions to someone with the appropriate authority and experience, commencing with your line manager. If this does not lead to a satisfactory response, then consider escalating the concern.

• Do deal with the matter promptly. Any delay could cost the University money or reputational damage. If in doubt, report your suspicions anyway.

• Do not be afraid of raising your concerns. Your concerns will be dealt with in confidence. You will not be ridiculed and will not suffer any recriminations because of voicing a reasonably held suspicion.

• Do not confront an individual or individuals with your suspicions and don't accuse any individuals directly.

• Do not try to investigate the matter yourself. There are special rules surrounding the gathering of evidence for use in these cases. Any attempt to gather evidence by people who are unfamiliar with these rules may compromise the case.

• Do not tell anyone about your suspicions other than those with the proper authority. All reports will be investigated and if appropriate referred to the relevant bodies.

If you have any concerns or questions you can email: AML@salford.ac.uk

Appendix D: Guidance for line-managers

• Do be responsive to staff concerns. The University needs to encourage staff to voice any reasonably held suspicions as part of developing an anti-fraud culture. As a manager you should treat all staff concerns seriously and sensitively.

• Do note all relevant details. Get as much information as possible from the reporting member of staff. If the staff member has made any notes, obtain these also. In addition, note any documentary evidence that may exist to support the allegations made. But DO NOT interfere with this evidence in any way.

• Do advise the appropriate person according to this policy.

• Do deal with the matter promptly.

• Do not ridicule suspicions raised by staff. The University cannot operate effective anti-fraud and whistle blowing policies if staff are reluctant to pass on their concerns to management.

• Do not approach or accuse any individuals directly.

• Do not convey your suspicions to anyone other than those with the proper authority.

• Do not try to investigate the matter yourself. Remember that poorly managed investigations by staff who are unfamiliar with evidential requirements are highly likely to jeopardise a successful outcome.

Appendix E: Suspicious Activity Report

CONFIDENTIAL – Suspicious Activity Report *Please complete and send this to the MLRO using the details below*	
From:	School/Professional Service:
Contact Details:	
DETAILS OF SUSPICIOUS ACTIVITY [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 you 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:
Please do not discuss the content of this report with anyone you believe to be involved in the suspected money laundering activity described.	

Appendix F: MLRO Report

MLRO Report (to be completed by MLRO)	
Date Report Received	Date Report acknowledged
Consideration of Disclosure:	
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? Yes / NO	
If YES record the date reported to NCA	
If consent required from the NCA to proceed with a potentially suspicious transaction? YES / NO If YES please confirm full details below:	
If Suspicious Activity Report is not reportable to National Crime Agency, set out below the reasons for non-disclosure.	
Signed:	Date: