



University of
Salford
MANCHESTER

Anti-Money Laundering Policy

Version Number 3.0

Effective from October 2023

Author: Executive Director of Finance

Document Control Information			
Revision History incl. Authorisation:			
Author	Summary of changes	Version	Authorised & Date
Ian Dempsey	<i>Formalises an existing internal policy that has been written using the BUFDG template.</i>	1	Approved at ARC 11 th June 2020
Ian Dempsey	<i>Highlight that this applies to subsidiary companies</i>	2	Highlighted by ARC September 2020
Ian Dempsey	<i>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.</i>	3	ARC June 2022
Policy Management and Responsibilities:			
Owner	This policy is issued by the Executive Director of Finance who has the authority to issue and communicate policy on financial matters of the University. The Executive Director has delegated day to day management and communication of the policy to the Treasury Management Team.		
Others with responsibilities (please specify):	All subjects of the Policy will be responsible for engaging with and adhering to this policy.		
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		
Consultation:			
Staff Trades Unions via HR Students via USSU Relevant external bodies (specify)	N/A		
Review:			
Review due:	Bi-Annually with report back to ARC every two years by July 2024		
Document location:			
University of Salford Finance Policies page			
The owner and author are responsible for publicising this policy document.			

1. Purpose

The purpose of this document is to make all staff and students of the University aware of the strict money laundering policy that the University follows. 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. Definitions & Legislative Context

The Money Laundering, Terrorist Financing & Transfer of Funds Regulations 2017 (MLR 2017) came into force on 26 June 2017. They implement the EU's 4th Directive on Money Laundering. In doing so, they 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.

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 stages in money laundering: placement, layering and integration. Placement is where the proceeds of criminal activity enter into the financial system; layering distances the money from its illegal source through layers of financial transactions; finally, integration involves the re-introduction of the illegal proceeds into legitimate commerce by providing an apparently genuine explanation for the funds.

3. Scope

This policy applies to all members of the University and subsidiary companies including staff, students and to third parties, including academic partners, undertaking business on behalf of the University and its subsidiary companies.

Money laundering is a criminal offence. In the UK, penalties include unlimited fines and/or terms of imprisonment ranging from two to 14 years.

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:

- i) conceal, disguise, convert or transfer criminal property or to remove it from the United Kingdom;
- ii) enter into an arrangement that you know or suspect makes it easier for another person to acquire, retain, use or control criminal property; and
- iii) 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.

Defences

In all three cases, they will have a defence if they made a so-called *authorised disclosure* of the transaction either to the Nominated Officer or to National Crime Agency and the National Crime Agency does not refuse consent to it.

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 (s)he received the information.

The Offence of Prejudicing Investigations / Tipping-Off

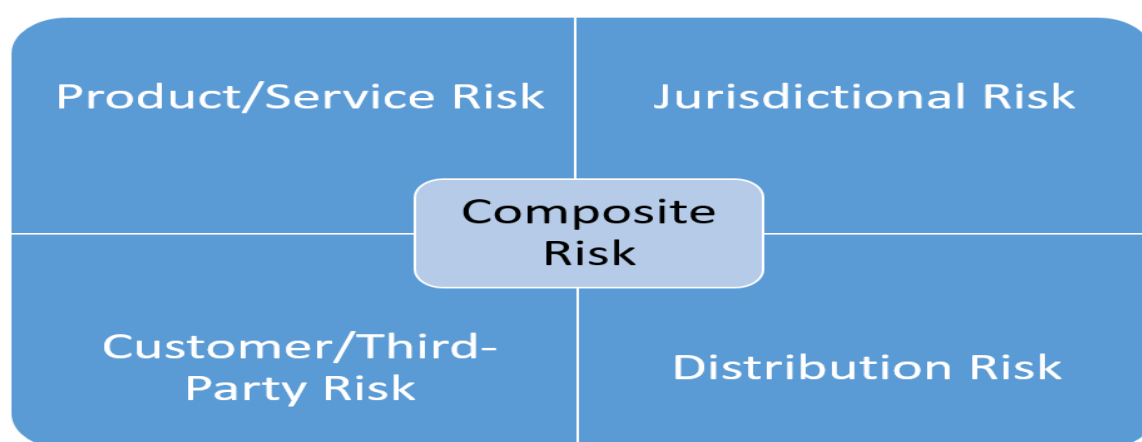
The purpose of making an authorised disclosure to the National Crime Agency is to allow it to investigate the suspected money laundering so it can decide whether to refuse consent to the transaction. That investigation would be compromised if the person concerned (or indeed anyone else) were to be told 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 the University's procedures may be taken against members of staff who fail to comply with this policy.

4. Risk Assessment

MLR 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.

Possible signs of money laundering include:

- a) large unexpected payments;
- b) multiple small payments to meet a single payment obligation;
- c) payments or prospective payments from third parties, particularly where:
 - a. there is no logical connection between the third party and the student, or
 - b. where the third party is not otherwise known to the University, or
 - c. 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 particular 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.

5. Risk Mitigation

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>

6. 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.

7. 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 no longer accept cash payments for tuition fees.

The Universities 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.

8. Know Your Customer /Supplier

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 including date of birth and home address. For third parties’ letters or documents proving name, address and relationship should be obtained.

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.

9. 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. Financial Sanctions Targets

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 undertake any research or consultancy activities with entities and/ or individuals in any of the following countries:

- Afghanistan
- Belarus

- Burma
- Burundi
- Central African Republic
- Democratic republic of Congo
- Egypt
- Iran
- Iraq
- Libya
- Mali
- Nicaragua
- North Korea
- Republic of Guinea
- Republic of Guinea – Bissau
- Russia
- Somalia
- South Sudan
- Syria
- Tunisia
- Turkey
- Ukraine
- Venezuela
- Yemen
- Zimbabwe

please consult with either the MLRO or his deputy so that the University can review the register and ensure that the proposed activity is not with an embargoed individual or organisation.

11. Roles and Responsibilities

The Director of Finance has responsibility for the Anti- Money Laundering Policy, which will be reviewed by the Audit and Risk Committee.

12. 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
Deputy Director of Finance
Email: A.Crozier@salford.ac.uk

And the deputy is:

Ian Dempsey
Head of Financial Accounting
Telephone 0161 295 4439
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.

13. 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 Annex A. 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.

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 3.

The MLRO will report any findings to the Director of Finance who will carry out any investigation in accordance with the Counter Fraud Policy and Response Plan.

14. 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.

15. Related Policies

The following related documents can be found at:

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

Financial Regulations

Counter Fraud Policy

And the Whistle Blowing Policy at:

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

16. Review, Approval and Publication

The Anti- Money Laundering Policy is subject to review every 3 years by the Director of Finance 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.

Annex A: Suspicious Activity Report

CONFIDENTIAL – Suspicious Activity Report <i>Please complete and send this to the MLRO using the details below</i>	
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 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 you believe to be involved in the suspected money laundering activity described.</i>	

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: