Anti-Money Laundering & Terrorist Financing Policy

Responsibility for Policy:	Finance Director
Relevant to:	All LJMU Staff, Governors, Contractors
Approved by:	Audit & Risk Committee, June 2023
Responsibility for Document Review:	*As above and/or designated member of their team.*
Date introduced:	November 2011
Date(s) modified:	June 2023
Next Review Date:	June 2024

RELEVANT DOCUMENTS

External Legislation

- Proceeds of Crime Act 2002 (as amended)
- Terrorism Act 2000 (as amended by the Anti-terrorism, Crime and Security Act 2001)
- Counter-terrorism Act 2008
- 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)

RELATED POLICIES & DOCUMENTS

- Treasury Management Policy
- Anti-Slavery & Human Trafficking Policy
- Financial Due Diligence Policy
- Staff Disciplinary Procedure and Code of Conduct
- Anti-Bribery Policy

LJMU Training modules

- Anti-Money Laundering Module

Anti- Money Laundering & Terrorist Financing Policy

1. Purpose

The purpose of this document is to make all LJMU Staff, Governors, Contractors of the University aware of the strict money laundering policy that Liverpool John Moores (the University) follows. The University is committed to the highest standards of openness, transparency, accountability, and to conducting its affairs in accordance with the requirements of the relevant funding and regulatory bodies. The University has a zero-tolerance approach to money laundering.

This policy sets out the respective obligations of the University and its staff. It also sets out the procedure to be followed if money laundering is suspected and defines the responsibility of individual employees in the process.

This policy forms part of the **Financial Regulations**.

2. Scope

This policy applies to the University and all its subsidiary undertakings and all those working for it, whether as an officer, employee, worker, intern, secondee, subcontractor, Governor, agent or in any other capacity (for the purposes of this Policy, collectively referred to as "Staff").

Any failures to adhere to this policy may be dealt with under the University's Staff Disciplinary Policy or Staff Performance Management Policy as appropriate. Note that any such failures also expose the individual concerned to the risk of committing a money laundering criminal offence.

3. Definitions & The Legislative Context

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** is where the proceeds of criminal activity enter into the financial system;

- **Layering** which distances the money from its illegal source through layers of financial transactions;
- **Integration** which involves the re-introduction of the illegal proceeds into legitimate commerce by providing an apparently genuine explanation for the funds.

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

- Failing to report knowledge and or suspicion of money laundering
- Failing to have adequate procedures to guard against money laundering
- Knowingly assisting money launderers
- 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, imposed by HM Revenue and Customs (HMRC) and /or the Financial Conduct Authority (FCA).

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 Proceeds of Crime Act 2002;
- the prejudicing investigations offence under the Proceeds of Crime Act 2002; 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 Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.

The Principal Money Laundering Offences

These offences, contained in sections 327, 328 and 329 Proceeds of Crime Act 2002, apply to any property (e.g. cash, bank accounts, physical property, or assets) that constitutes a person's benefit from criminal conduct or any property that, directly or indirectly, represents such a benefit (in whole or partly) where the person concerned knows or suspects that it constitutes or represents such a benefit. 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;
- enter into an arrangement that you know or suspect makes it easier for another person to acquire, retain, use or control criminal property; and
- 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, staff will have a defence if they made a so-called authorised disclosure of the transaction either to the **Nominated Officer** or to the National Crime Agency and the National Crime Agency does not subsequently refuse consent to that transaction.

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 a money laundering investigation. University staff can commit this offence if they tell a person an authorised disclosure has been made in their case.

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

These regulations are aimed at protecting the gateway into the financial system. They apply to a range of businesses all of which stand at that gateway. They require these businesses to conduct money laundering risk assessments and to establish policies and procedures to manage those risks. Businesses to which the regulations apply are specifically required to conduct due diligence of new customers, a process known as “Know your Customer” or “KYC”. There are criminal sanctions, including terms of imprisonment of up to two years, for non-compliance. Whilst the University is not covered by the regulations in its work as a provider of education, the regulations provide a guide to the management of risk in handling money and due diligence is at the heart of the University’s approach in this policy to managing risk.

Terrorist Finance

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 a number of 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.

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.

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.

4. 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. For example:

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

- where 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 politically exposed persons ("PEP");
- 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 or wealth or reason for payment;
- prospective payments from a potentially risky source or a high-risk jurisdiction;
- the payer's ability to finance the payments required is not immediately apparent or the funding arrangements are otherwise unusual.
- An individual or company attempts to engage in "circular transactions" where a payment is made to the University followed by an attempt to obtain a refund.
- 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)
- 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".
- Involvement of an unconnected third party in a contractual relationship without any logical explanation.

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

5. Liverpool John Moores Procedures

The University has a number of policies and procedures in place to minimise the risk of money laundering:

5.1 General Overview

The University will:

- conduct an annual 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 policies and 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 Nominated Officer to be responsible for reporting any suspicious transactions to the National Crime Agency;
- provide training to all relevant members of staff, including temporary staff, on joining the University, and provide annual refresher training; and
- maintain and retain full records of work done pursuant to this policy.

5.2 Roles and Responsibilities

Finance Director

The **Finance Director** has responsibility for the Anti- Money Laundering & Criminal Finances Act Policy, which will be reviewed by the **Audit and Risk Committee**.

The Finance Director will ensure:

- annual (more frequently if circumstances change) assessments of the University's money laundering and terrorist finance risks are conducted and relied on to ensure the effectiveness of this policy;
- appropriate due diligence is conducted, as a result of which risks relating to individual transactions are assessed, mitigated and kept under review;
- anti-money laundering and counter-terrorist finance training is delivered within the University, including training on this policy, with records of attendance maintained; and
- this policy is kept under review and up-dated as and when necessary and levels of compliance are monitored.

To facilitate the review and accountability functions, the Finance Director will ensure:

- the availability of appropriate management information to permit effective oversight and challenge; and

- the maintenance and retention of full records of work done under this policy. The University will retain all anti-money laundering and counter-terrorist finance records securely for a period of at least five years.

Nominated Officer

The Nominated Officer is the primary contact for any further information or to report any suspicious activity. ***The nominated officer is the University Secretary and General Counsel***

The Nominated Officer is responsible for:

- receiving reports of suspicious activity;
- 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 National Crime Agency by completing and submitting a Suspicious Activity Report;
- asking the National Crime Agency for consent to continue with any transactions that must be reported and making sure that no transactions are continued illegally.
- Recording in writing the reasons for their decision and retain that record centrally. Information that an authorised disclosure has been made must never be kept on the file relating to the person concerned.

Staff

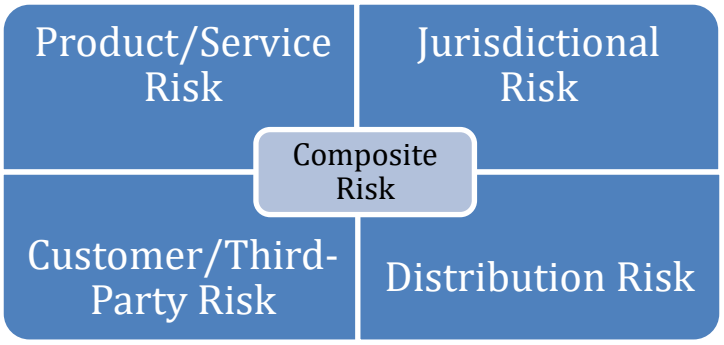
All Staff are responsible for reporting suspicious activity

- Money laundering legislation applies to all Staff.
- Staff who needs to report suspicious activity must complete the Suspicious Activity Report (SAR) which is detailed in **Appendix 1.**
- Staff could be committing an offence if they suspect money laundering (or if they become involved in some way) and do nothing about it.
- 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.

5.3 Risk Assessment

A risk assessment will be performed at a minimum annually, more frequently should circumstances change.

The risk assessment will consider 4 main areas



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

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

Customer/Third-Party Risk 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 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.

5.4 Due Diligence Processes

The University has a separate **Financial Due Diligence Policy.**

Financial due diligence is considered as part of bidding for research, consultancy and collaborative provision and also when considering collaborative partnerships.

5.5 Know Your Customer (KYC)

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" requirement 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. This is why it is important for staff to comply with this policy (and other applicable Finance policies) when engaging with any third party on behalf of the University.

5.6 Politically Exposed Persons (PEP) Checks

A **politically exposed person (PEP)** is someone who has been appointed by a community institution, an international body or a state, including the UK, to a high-profile position within the last 12 months.

Under anti-money laundering regulations, the main aim of applying additional scrutiny to work involving PEPs is to mitigate the risk that the proceeds of bribery and corruption may be laundered, or assets otherwise stripped from their country of origin.

PEPs can be:

- heads of state,
- heads of government, ministers, and deputy or assistant ministers
- members of Parliament
- members of courts of auditors or of the boards of central banks
- ambassadors, chargés d'affaires and high-ranking officers in the armed forces
- members of the administrative, management or supervisory bodies of state-owned enterprises
- members of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not generally subject to further appeal, except in exceptional circumstances

PEPs also include:

- the person's family members
- close business associates
- beneficial owners of the person's property (someone who enjoys the benefits of ownership even though the title of the property is in another person's name)

The University will use information that's reasonably available to help identify PEPs, including:

- public domain information, such as parliament and government websites
- reliable public registers, such as the Companies House 'register of companies' and 'people with significant control register'
- commercial databases that contain lists of PEPs, family members and known close associate

5.7 Financial Sanctions Checks

The UK government publishes frequently updated guidance on financial sanctions targets, which includes a list of all targets. This guidance can be found at:

The UK Sanctions List - GOV.UK (www.gov.uk)

The sanctions list is checked as part of the University's due diligence procedures by the Finance Team.

5.8 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.

5.9 Cash

The University is cashless and does not accept or receive cash payments.

5.10 Training

- On joining the University any staff whose duties will include undertaking a finance function will receive anti-money laundering training as part of their induction process.
- All staff undertaking a finance function will receive annual refresher anti-money laundering and counter-terrorist finance training.
- 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 for at least five years records of its anti-money laundering and counter-terrorist financing training.