BIRKBECK, UNIVERSITY OF LONDON

ANTI-MONEY LAUNDERING POLICY

This policy was approved by Finance & General Purposes Committee at its meeting on 4 June 2024

1. INTRODUCTION

1.1 Birkbeck is committed to upholding the highest standards of openness, transparency, probity and accountability. The University seeks to conduct its affairs in a responsible manner, taking into account responsibilities as a public body, the requirements of the funding bodies, government legislation.

1.2 The University will 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 the University. 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.

1.3 Birkbeck does not tolerate activities that may facilitate money laundering, corruption, fraud, or dishonesty.

1.4 Other relevant policies that should be read in conjunction with this policy are:

Financial Regulations
Philanthropic Gift and Acceptance Policy
Anti-Bribery Corruption Policy
Whistleblowing Policy
HR Code of Conduct for Managing Conflicts of Interest

2. SCOPE and PURPOSE

2.1 The primary objective of this policy is to safeguard the University's financial assets and reputation by detecting and preventing money laundering activities. It is also to raise awareness of people working for and with the University to be able to recognise when money laundering may be taking place and what action to take to prevent that in the first instance, or to deal with it should it arise.

2.2 This policy outlines how the University manages money laundering risks and complies with its legal obligations.

2.3 The University must be able to demonstrate that it has effective procedures in place that mitigate the risk of being implicated in money laundering activities.

2.4 This policy applies to all employees of the University. It extends to all financial transactions and activities conducted by or on behalf of the University in the UK or overseas.

3. WHAT IS MONEY LAUNDERING?

3.1 Money laundering is the process of concealing the origin and ownership of the proceeds of crime and corruption by transforming these proceeds into what appear to be legitimate assets. It takes ‘dirty funds’ generated through illicit activity and converts them into other apparently lawful assets, therefore ‘cleaning’ them. In addition, most anti-money laundering (AML) laws that regulate financial systems link money laundering (which is concerned with the source of funds) with terrorism financing (which is concerned with the destination of funds).

3.2 Money laundering schemes come with varying levels of sophistication from the very simple to the highly complex. Straightforward schemes can involve cash transfers or large cash payments whilst the more complex schemes are likely to involve the movements of money across borders and through multiple bank accounts.

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

- Placement - when the proceeds of crime enter the financial system.
- Layering - the process of distancing the proceeds from its original criminal source through layers of financial transactions.
- Integration - when the criminal proceeds are then used in some way, appearing to be from a legitimate source.

3.4 In the UK, the approach to money laundering is generally based on objectives that are specified in legislation and/or Financial Conduct Authority (FCA) rules. These objectives will often be a requirement of an EU Directive and subsequently incorporated into UK law.

3.5 Key elements of the UK AML framework that apply to universities include:

- Proceeds of Crime Act 2002 (as amended)
- Terrorism Act 2000 (as amended by the Anti-terrorism, Crime and Security Act 2001)
- Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017)
- Counter-terrorism Act 2008, Schedule 7
- HM Treasury Sanctions Notices and News Releases
- Joint Money Laundering Steering Group (JMLSG) Guidance
- Sanctions and Anti-Money Laundering Act 2018

4. MONEY LAUNDERING OFFENCES

4.1 The Money Laundering and Terrorist Financing 2019 legislation outlines several offences including:

- failing to report knowledge 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.

4.2 The penalties for breaching money laundering legislation are severe. Individuals connected with any stage of money laundering could face unlimited fines and / or prison terms ranging from 2 to 14 years, depending on the offence. 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).

4.3 Potentially any member of staff could be committing an offence under the money laundering laws if they suspect money laundering or if they become involved in some way and do nothing about it.

4.4 Staff who do not report suspicious activity in line with this policy may face disciplinary action and may be personally liable to prosecution.

5. RISK

Risk Assessment

5.1 Money laundering regulations require the University to assess its operations and activities regarding the potential exposure to money laundering. There are four main areas of risk that need to be considered, these are:

- Product/Service Risks associated with our standard product and service offerings (for example teaching and research activities).
- Jurisdictional Risks associated with geography, location and jurisdiction including, but not limited to, the University's countries of operation, the location of customers (including our students), suppliers and agents.
- Customer/Third Party Risks associated with the people and/or organisations that we undertake business with. This could be students, customers, suppliers, and anyone else who has a contractual relationship with the University.
- Distribution Risks associated with how we undertake business, including direct and indirect relationships (for example via an agent or third party), face to face, online or by telephone.

Identifying Risks

5.2 The University is required to have appropriate systems and internal control mechanisms to mitigate the risk of money laundering. Typical risks may include the following:

Potential risk	**Response**
Large cash payments, or multiple small cash payments to meet a single payment obligation.	Cash payments are not accepted. Any attempt to pay in cash is refused and the payer is asked to use an alternative payment method.
Unusual or large payments are made into the University bank accounts from a potentially risky source or a high-risk jurisdiction.	The University will make every effort to establish what the payment is for. The University bankers also advise on high-risk countries where financial transactions are either prohibited or heavily restricted. The University does not advertise its bank details the website or provide them to unknown sources by telephone or email to ensure unknown payments are not transferred into the University's bank account.

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.	The University will only accept payments from students, sponsors, external funders (where a funding agreement is in place) or commercial debtors.
A series of small payments made from various credit cards with no apparent connection to the student and sometimes followed by chargeback demands.	Only transfers from students via one of the approved payment methods will be accepted. These are: TransferMate, Convera or Flywire. All online payments are made via a secure third-party. These third-party platforms do not accept payments from sanctioned countries or individuals.
Donations which are conditional on individuals or organisations, who are unfamiliar to the University, being engaged to carry out work.	The due diligence is detailed in the Philanthropic Gift and Acceptance Policy.
A prospective payer who wants to pay up-front a larger sum than is required or otherwise wants to make payment in advance of them being due.	The University does not accept advance payments for sums greater than is required. Tier 4 deposits are requested in advance from international students and are subject to other AML controls.
Prospective payers who are obstructive, evasive, or secretive when asked about their identity or the source of their funds.	The University only accepts payment from students or certified sponsors. Payers are required to follow the University's due diligence processes.
The payer's ability to finance the payments required is not immediately apparent or the funding arrangements are otherwise unusual.	Any payment plans which are not in line with University policy are approved by the Income Team. The Income Team do not accept payment proposals which appear suspicious in terms of affordability or source of funding.
A person or company undertaking business with the University failing 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.)	The supplier approval process includes a credit check and a check of details at Companies House (if applicable). Suppliers that fail this will not be approved. Suppliers that fail to state information such as company or VAT registration number (where applicable) will be contacted by the Payments team who will investigate the supplier further.
A potential supplier who 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."	The University does not have to accept the lowest, or any, tender. Where a very low tender is received the Procurement Manager will undertake checks to ascertain why. This information is documented as part of the tender process.
Requests for refunds of advance payments, particularly where the University is asked to make the refund payment to someone other than the original payer.	Refunds will only be made back to source, and to the original payer. The Income Team will undertake appropriate checks before any refund is processed to verify the identity of the person, the

	reason and that it has been properly authorised.

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 (MLRO), named at the end of this policy.

6. MONITORING AND COMPLIANCE

Due diligence

6.1 Due diligence is the process by which the University assures itself of the origin of the funds it receives and that it can be confident 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 funds are received. Funds must not be returned before due diligence has been reviewed.

6.2 In practical terms this means:

- Identifying and verifying the identity of a payer, typically a student, corporate customer or a donor.
- Knowing where the payment is to come from or in cases of payments made by a third party on behalf of the student or donor, identifying and verifying the identity of that third party.
- Identifying and verifying the source of funds from which any payment to the University will made.

Know Your Customer

6.3 Anti-Money Laundering regulations require that the University must be reasonably satisfied as to the identity of the customer that they are engaging with in a contractual relationship. To discharge the “reasonably satisfied” requirement the University must for example have obtained a minimum level of personal information from a student before entering into a contract.

6.4 The University has a robust "know your customer" process for students and other customers, especially overseas students and those from high-risk areas (those named in the UK Government's sanctioned list). For students this includes checking a student’s:

- passport
- visa
- birth certificate
- correspondence to verify their home address.

6.5 Third-party sponsors are required to complete a sponsor form. On review, if the organisation is not known to the University a Companies House check will be undertaken to verify the validity of the potential customer. This check is also carried out on new commercial customers.

6.6 For organisations not known to the University (suppliers and commercial debtors) these checks include:

- Checking for letter-headed documents
- Checking websites
- Requesting credit checks

- Meeting key contacts/sponsors to verify validity of contact.

Financial Sanctions Targets

6.7 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/the-uk-sanctions-list. The list provides information to assist in deciding whether the University is dealing with someone who is subject to sanctions. The Income Team review this list regularly to ensure the University has no relationship with any individuals on this list. Evidence of this review by the Income Team is recorded and retained (person completing the check and date).

Training

6.8 The Director of 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.

7. ROLES AND RESPONSIBILITIES

7.1 The role of the MLRO is to be aware of any suspicious activity in the University which might be linked to money laundering or terrorist financing, and if necessary, to report it. They are specifically responsible for:

- Receiving reports of suspicious activity from any employee of the University and maintaining a register of all reports;
- Considering all reports and evaluating whether there is, or seems to be, any evidence of money laundering or terrorist financing;
- Reporting of all reports received, whether potential or actual cases of money laundering to the Vice Chancellor;
- Reporting any suspicious activity or transaction(s) to the National Crime Agency (NCA) by completing and submitting a Suspicious Activity Report;
- Asking the NCA for consent to continue with any transactions that they have reported and ensuring that no transactions are continued illegally.

7.2 The designated MLRO for the University is the Director of Finance (Keith Willett).

7.3 All employees of the University have an obligation to report any suspicious activity to the MLRO. It is an offence under the current legislation to fail to report / have knowledge of money laundering activity.

8. DISCLOSURE PROCEDURE FOR INDIVIDUALS

8.1 Employees that suspect money laundering activity is taking or has taken place or are concerned that their involvement in a transaction may amount to a breach of the regulations must disclose this immediately to their line manager. If in consultation with the line manager reasonable suspicion is confirmed a disclosure report must be made to the MLRO.

8.2 This disclosure should be made on the proforma report attached at Appendix 1 and should be completed the same day the information came to the employee's attention.

8.3 Employees that do not disclose in line with this policy may be personally liable to prosecution under the regulations.

8.4 The report should include as much detail as possible including:

- Full available details of the people (including the person reporting), companies involved, and other members of staff if relevant.
- Full details of transaction and nature of each person's involvement in the transaction.
- Suspected type of money laundering activity or use of proceeds of crime with exact reasons as to why the individual reporting is suspicious.
- The dates of any transactions, where they were undertaken, how they were undertaken and the likely amount of money or assets involved.
- Any other information that may help the MLRO judge the case for knowledge or suspicion of money laundering and to facilitate any report to the National Crime Agency (NCA).

8.3 Once reported to the MLRO employees must follow any instructions provided. Employees must not make any further enquires unless instructed to do so by the MLRO. At no time and under no circumstances should the employee voice any suspicions to the person(s) suspected of money laundering. If appropriate the MLRO will refer the case to the National Crime Agency (NCA) who will undertake any necessary investigation. This may include consent to continue with a particular transaction and care should be taken not to 'tip off' the individuals concerned, otherwise the individual may be committing a criminal offence.

9. REVIEW, APPROVAL AND PUBLICATION

9.1 The Anti- Money Laundering Policy is subject to review every three years or following a change to relevant UK legislation.

Date of last Review: June 2024
Date of Next Review: June 2027