Anti-Money Laundering Policy

1. Introduction and purpose

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).

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.

Apparently legitimate, normal transactions, such as the payment of student fees followed by a refund, could be used to conceal money laundering. It is therefore essential that the College has appropriate policies and procedures in place to ensure it does not inadvertently legitimise suspicious individuals or transactions.

1.1. Money laundering legislation

In addition to the money laundering offences under the Proceeds of Crime Act 2002, the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017) came into force on 26 June 2017, implementing the EU's 4th Directive on Money Laundering.[1] A key difference in MLR 2017 legislation is that the College is required to adopt a more risk-based approach towards anti-money laundering, and in how it conducts due diligence.

In the UK, severe penalties are imposed on those connected with any stage of laundering money, including unlimited fines and/or terms of imprisonment up to 14 years.

It is a crime to:

i) conceal, disguise, convert or transfer criminal property or to remove it from the United Kingdom;

[1] In addition to this, key elements of the UK AML framework that apply to universities include: Terrorism Act 2000; Counter-terrorism Act 2008; Schedule 7 HM Treasury Sanctions Notices and News Releases and; Joint Money Laundering Steering Group (JMLSG) Guidance

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.

College staff could be committing the following offences:

- 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.

College staff will have a defence if they made a so-called *authorised disclosure* of a transaction either to the Nominated Officer (see below) or to National Crime Agency. 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.

1.2. Terrorist financing legislation

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 College 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:

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.

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 this policy.

2. Scope

This Policy sets out the College's position with regard to money laundering and outlines how the College mitigates money laundering risks, the roles and responsibilities of College staff, and the College's training and reporting requirements.

3. Policy statement

Royal Holloway, University of London and its subsidiary are committed to the highest standards of ethical conduct throughout their activities in the UK and overseas. Therefore the College will adopt systems and controls to mitigate any financial crime risks in order to provide reasonable assurance that the College's policies and procedures will prevent and detect money laundering.

A risk-based assessment has been carried out to identify and assess areas of risk in relation to money laundering and terrorist financing, and which incorporates appropriate procedures such as Know Your Customer (KYC) / Customer Due Diligence (CDD), and it will be kept up-to-date (see Appendix 1).

The College's policies and procedures will be periodically reviewed and tailored to ensure that they take account of the various controls required to address the risks associated with its operations, products and services and those with whom the College transacts.

3.1. Warning signs

Payments or prospective payments made to or asked of the College can generate a suspicion of money laundering for a number of different reasons. For example:

i) large cash payments;
ii) multiple small cash payments to meet a single payment obligation;
iii) 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 College, or
    c. where a debt to the College is settled by various third parties making a string of small payments;
iv) payments from third parties who are foreign public officials or who are politically exposed persons ("PEP");
v) payments made in an unusual or complex way;
vi) 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 College is allowed to retain interest or otherwise retain a small sum;
vii) donations which are conditional on particular individuals or organisations, who are unfamiliar to the College, being engaged to carry out work;
viii) requests for refunds of advance payments, particularly where the College is asked to make the refund payment to someone other than the original payer;
ix) a series of small payments made from various credit cards with no apparent connection to the student and sometimes followed by chargeback demands;
x) 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;

xi) prospective payers are obstructive, evasive or secretive when asked about their identity or the source of their funds or wealth;
xii) prospective payments from a potentially risky source or a high-risk jurisdiction;
xiii) the payer's ability to finance the payments required is not immediately apparent or the funding arrangements are otherwise unusual.

4. Roles and responsibilities

All staff and Council Members are subject to anti-money laundering legislation and must be vigilant regarding the risk of financial crime and fraud. Potentially, any member of staff could be committing an offence if they suspect money laundering or become involved in some way and do nothing about it. Failure to comply with this policy and the obligations detailed in this policy may result in disciplinary action for staff.

The College is required to appoint a Nominated Officer to be aware of any suspicious activity in the organisation that might be linked to money laundering or terrorist financing, and if necessary to report it. The Nominated Officer will be the Chief Financial Officer and the deputy will be the Head of Financial Control.

5. Related documents

This policy should be read in conjunction with the following documents:

- Financial Regulations
- Criminal Finances Act Policy
- Donations Acceptance Policy
- Anti-Fraud Policy
- Anti-Bribery Policy
- Procurement Policies and Procedures
- Whistleblowing Policy

6. Monitoring and compliance

6.1. Due Diligence

Due diligence is the process by which the College 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 College 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.

In practical terms this means:

i) identifying and verifying the identity of a payer or a payee, typically a student or a donor;
ii) where the payment is to come from or to be made by a third party on behalf of the student or donor, identifying and verifying the identity of that third party;
iii) identifying and verifying the source of funds from which any payment to the College will be made; and
iv) identifying and in some circumstances verifying the source of wealth from which the funds are derived.

6.2. Reporting

The College will take all reasonable steps to identify and report suspicious transactions, of all types. Appropriate due diligence will be conducted, as a result of which risks relating to individual transactions are assessed, mitigated and kept under review.

Any member of staff who is exposed to any suspicious activity must report this promptly to the Nominated Officer using the Reporting Form at Appendix 4. Individuals must cooperate fully with any ensuing investigations and must maintain confidentiality about any suspected incidents.

Upon receipt of any reports of suspected money laundering the Nominated Officer will consider all the information available, including a review of transactions, the length of any business relationship, the pattern of interactions, one-off transactions, changes in the types of transactions and so on, and will make all other reasonable enquiries as they see fit, to determine whether or not there is suspicion of money laundering. The Nominated Officer will report externally if appropriate, to the National Crime Agency or make a disclosure under the Terrorism Act 2000, as soon as practicable after the report was received. The Nominated Officer will act reasonably and in good faith and will not report suspicions as a matter of routine without undertaking reasonable enquiries. The Nominated Officer will record in writing the reasons for their decision and retain that record centrally for at least five years. Information that an authorised disclosure has been made must never be kept on the file relating to the person concerned.

No member of staff may reveal to any person outside the relevant department, including specifically the student or third party funder in question, that an authorised disclosure or a disclosure under the Terrorism Act 2000 has been made.

6.3. Tipping off or prejudicing an investigation

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. College staff can commit this offence if they tell a person an authorised disclosure has been made in their case. This policy requires authorised disclosures to be kept strictly confidential.

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. At paragraph 35 below, this policy requires disclosures under the Terrorism Act 2000 to be kept strictly confidential.

6.4. Training

All relevant members of staff (i.e. those who handle transactions which may involve money laundering, or manage those who do) will receive regular training in this policy and the wider aspects of AML, including at induction. For the purposes of the College this means staff who work in the

Finance Department, Development Alumni Team (donations), Student Fees team, Student Administration team, Academic School/Department Managers, Professional Service Administrators involved in regularly raise Sales Orders, such as Commercial Services and Estates.

6.5. Record keeping

The College will take reasonable care to make and keep adequate records (including customer identification and accounting records) which are appropriate to the scale, nature and complexity of its business. These records typically include identity documents, transaction records, records of reports (internal and external), and training records. These records will be kept according to College data retention protocols but this will be at least five years from the date they are relied upon.

7. Document Control Information

Policy Owner	Chief Financial Officer
Operational Owner	Head of Financial Control
Approving Body	Council
Date of Approval	1 July 2021
Related Policies and procedures and guidelines	Counter-fraud Anti-Bribery Criminal Finances Act Financial Regulations Procurement policies and procedures Whistleblowing
Reviewed by	Executive Board Finance Committee
Approved by Finance Committee	10/6/2021
Deadline for Review by Council	July 2023

Version History		
Version (newest to oldest)	Date of approval	Summary of changes
Version 2	1 July 2021	Various additions based on sector guidance
Version 1	28 February 2019	

Appendix 1 Anti-Money Laundering Risk Assessment – not for publication (available on request)

Appendix 2: Know Your Customer (KYC) and Customer Due Diligence (CDD)

The College must be reasonably satisfied as to the identity of the customer (and others). Know Your Customer (KYC) is the Customer Due Diligence (CDD) that the College must perform in order to identify its business relationships and customers and therefore ascertain relevant information pertinent to continuing to do business. As well as ensuring the College complies with the law, these procedures help to ensure that the College does not enter into student and other relationships that might be considered too risky.

There are essentially three components that make up the CDD measures required by the Money Laundering Regulations. The three components are:

1. Ascertaining and verifying the identity of the customer/student i.e. knowing who they are and confirming that their identity is valid by obtaining documents or other information from sources which are independent and reliable. For example, student identity checks include obtaining a copy of photo-identification (such as a passport, photocard driving licence or other National Identity card) to confirm their name, date of birth and nationality. Overseas students must provide the appropriate passport and visa documentation under UK Visas and Immigration (UKVI) regulations.

2. Ascertaining and verifying (if appropriate) the identity of the beneficial owners of a business, if there are any, so that the identity of the ultimate owners or controllers of the business is known. For example, all company sponsorships must be confirmed on company headed paper and include the names of owners/directors of the company.

3. Information on the purpose and intended nature of the business relationship i.e. knowing the nature of the engagement and why it exists.

The level of due diligence carried out will be determined by a risk-based approach, considering factors such as the nature of the service being sought and the length and nature of any existing relationship. The College ensures the CDD records relied on are retained for five years from the date on which reliance commences. Failure to do so is a criminal offence.

Appendix 3 Financial Sanctions Targets

Financial sanctions are imposed by the UK and other governments and may apply to individuals, entities and governments, who may be resident in the UK or abroad. Financial sanctions orders prohibit an organisation or company from carrying out transactions with a person or organisation (known as the target). These measures can vary from the comprehensive - prohibiting the transfer of any funds to a sanctioned country and freezing the assets of a government, the corporate entities and residents of the target country - to targeted asset freezes on individuals/entities. 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

Appendix 4 - Suspected Money Laundering Reporting Form

CONFIDENTIAL - Suspected Money Laundering Reporting Form *Please complete and send to the Nominated Officer using the details below*	
Name:	Department:
Telephone number:	
DETAILS OF SUSPECTED OFFENCE [Please continue on a separate sheet if necessary]	
Name(s) and address(es) of person(s) involved, including relationship with the College:	
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:
Nominated Officer contact details: Contact name: Mary White Job title: Chief Financial Officer Phone number: 01784 443016 Email: Mary.White@rhul.ac.uk	
Please do not discuss the content of this report with anyone you believe to be involved in the suspected money laundering activity described. To do so may constitute a tipping off offence, which carries a maximum penalty of 5 years' imprisonment and/or an unlimited fine.	