Anti-Money Laundering Policy

Policy Owner	Secretary to Council
Approving Body	Council
Date of Approval	28 February 2019
Version number	1
Related Policies and procedures and guidelines	Counter-fraud Anti-Bribery Criminal Finances Act Financial Regulations Procurement policies and procedures Whistleblowing
Reviewed by	PRC Jan 2019
Approved by Audit and Compliance Committee	4/2/2019
Deadline for Review by Council	February 2021

1. Introduction

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).

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.

In the UK, severe penalties are imposed on those connected with any stage of laundering money, including 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 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.

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 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 risks associated with its operations, products and services and those with whom the College transacts.

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.

[1] In addition to this, key elements of the UK AML framework that apply to universities include: Proceeds of Crime Act 2002; Terrorism Act 2000; Counter-terrorism Act 2008; Schedule 7 HM Treasury Sanctions Notices and News Releases and; Joint Money Laundering Steering Group (JMLSG) Guidance

5. Reporting

The College will take all reasonable steps to identify and report suspicious transactions, of all types.

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, 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.

6. Training

All relevant members of staff (i.e. those who handle transactions which may involve money laundering, or manage those who do) will receive 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.

All new staff in relevant areas will be required to sign a record to verify that they have read and understood this policy.

7. 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.

8. Related policies and procedures

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

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

Appendix 1 Anti-Money Laundering Risk Assessment as at December 2018

The College is required to undertake a risk assessment, and to demonstrate and document that it was carried out and has been/will be kept up-to-date.

The College's AML controls and processes have to be in proportion to the financial crime risks and relate to the four primary sources of risks that, together, make up the College's composite risk:

- **Product/Service:** Risks associated with the College's standard products and services, including cash transactions, anonymous transactions, non-face-to-face transactions, transactions involving unknown third-parties and unregulated transactions (i.e. from unregulated third-parties).
- **Jurisdictional:** Risks associated with geography, location and jurisdiction including, but not limited to, the College's countries of operation, the location of customers, suppliers and/or agents, and transactional sources/destinations. Countries recognised to have inadequate AML controls and processes, countries subject to sanctions, embargoes and related measures and countries identified by recognised authorities as supporting terrorism and/or terrorist organisations.
- **Customer/Third-Party:** Risks associated with the people and/or organisations with whom the College undertakes business (in all forms), including customers/third-parties, agents, contractors, vendors and suppliers.
- **Distribution:** Risks associated with how the College undertakes business, including direct and indirect relationships (e.g. via an agent or third-party), face-to-face, digital/online and telephonic.

Examples where the risk of money laundering is heightened at the College may include (but are not limited to):

- Payment to the College of a substantial sum in cash, especially if there is not proper evidence of identity or address of the payer or even a complete absence of any legitimate source.
- Requests for student refunds by a third party or to a different account or method of payment to which the original payment was received.
- A person or organisation doing business with the College that lacks proper paperwork, e.g. company invoices with no registered office/number, exclusion of VAT, etc.
- Significant changes in the nature of transactions with a customer, e.g. size, frequency, etc
- An unusual pattern of sales orders followed by refunds.

Product/Service - Risk

The College's involvement in student loan finance will not normally present an opportunity for money laundering as funds are paid directly from the Student Loan Company (SLC) to the College, and the College is not responsible for processing loan repayments.

However the College receives educational loan funds for overseas students, for example from the US and India. The majority of US loans are from the US government's Department of Education, however there are some students who take out private loans with US banks. There are also a number of students who take out loans with private banks based in India.

Product/Service - Mitigation/Control

- Most risks are mitigated as SLC funds are paid direct to the College as the course provider, and any refunds are clawed back by the SLC directly.
- The US Department of Education loans are well regulated and any refunds are paid directly back to the US government.
- In the case of private loans from the US and India, the relationship is primarily between the student and the bank; any refunds are either paid directly to the bank account from which the funds were received, or in some cases directly to the bank who provided the loan.
- For any refunds paid to third party lenders, additional due diligence checks are made.
- Other than its relationship with the SLC, the College does not introduce students to lenders.

Given these factors, the Product/Service risk level for the College is **LOW.**

Jurisdiction - Risk - The current jurisdiction for the College covers both UK and overseas activities, with some of those overseas activities being undertaken in potentially higher-risk locations, where the College may partner with overseas organisations during research and related activities.

Jurisdiction - Mitigation/Control

- The Joint Money Laundering Steering Group (JMLSG) guidance clarifies that a presumption of low risk applies to UK or EEA/European jurisdictions unless the College's experience with certain types of customers within these jurisdictions calls for a higher risk factor to be applied.
- Whilst the College's experience relating to overseas activities more generally has not to date resulted in any significant concerns, ongoing vigilance will be required. See 'Third party' risk below for further detail.

Given these factors, the jurisdiction risk level for the College is **LOW**.

Customer/Third-Party - Risk - Most of the College's "customers" are residents in either UK or EEA countries. Many students pay online ("self-service") and the risk here is considered low as the account / credit card is traceable and payment is made via a Payment Service Provider (PSP).

Although the College has not experienced this, it is possible that students could deposit cash in a College bank account, which may heighten risk in the case of a refund request (as there is no source to which the refund can be verifiably made).

Some students come from and/or study in potentially higher-risk locations overseas. Tuition fees are also paid by sponsors, both in the UK and overseas (the vast majority of these are governmental although some are private). In particular there is a risk where refunds are requested by overseas students or their sponsors.

The College also receives material donations from third parties.

Customer/Third-Party – Mitigation/Control

- "Customer Due Diligence" (CDD) procedures are implemented to mitigate the potential customer risk (see Appendix 2 for more detail). Verification of individuals is undertaken using standard due diligence procedures such as specific identity checks and, for refunds, verifying the original account or card used to make the original payment. These are supported by further 'high-risk' (sanction) checks, for example for overseas sponsors. The former are performed routinely and automatically, whereas the latter is a manual check and only if a refund is requested.
- Following a payment by credit card or bank transfer, refunds are only made by the same method to the same account.
- No cash is accepted on the College campus for the payment of tuition or accommodation fees.
- Should a cash payment be made, for example by deposit into the College's bank account, additional checks would be made to verify the identity of any person or organisation requesting a refund. For higher risk transactions the College may consider using a third party specialist organisation to carry out additional due diligence checks on individuals or organisations.
- All organisations sponsoring students must be confirmed on company headed paper and include the names of owners/directors of the company.
- Sponsors are not invoiced until a student has completed enrolment, to reduce the need for any refunds; any sponsor overpayments or refunds are made directly back to the sponsor. Higher risk transactions may undergo additional checks using a third party specialist.
- In addition, payments from higher risk countries will be checked by the bank or the College's Payment Service Provider (PSP).
- Due diligence checks are carried out to determine the source of donations as laid out in the College's Donations Acceptance Policy.

Given these factors, the customer/third-party risk level for the College is **MEDIUM.**

Distribution - Risk - The College faces a number of risks associated with how it undertakes business, particularly where it is at a distance, or digital/online and telephonic only. The College has extensive international supplier/vendor relationships which creates a higher level of risk.

Distribution - Mitigation/Control

- Where an agent, third-party or representative is involved, the business relationship is only confirmed once the College has followed due process as outlined in the College's Procurement Policy and Procedures.
- If this fails to provide enough security, then consideration will be given regarding whether the relationship should continue and/or additional mitigating controls could be put in place.
- Checks include proof of bank details on headed paper, copy of a bank statement stating account name and details, certificate of incorporation, tax registration documentation, etc.

Given these factors, the distribution risk level for the College is considered to be **MEDIUM**.

Other controls in place to reduce money laundering risk include the following:

- The College has appointed a Nominated Officer – see section 4 of the Policy above.
- The College as a procedure for the reporting of suspicious activity – see section 5 of the Policy above, and Appendix 4.
- The College maintains adequate records of transactions – see section 7 of the Policy above.
- The College carries out regular risk assessments to identify areas of concern and operations that are most vulnerable to money laundering.
- The College carries out appropriate training for staff – see section 6 of the Policy above.

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, to satisfy the requirements, student identity checks for money laundering purposes include obtaining a copy of photo-identification (such as a passport, photocard driving licence or other National Identity card) to confirm their name and date of birth, and proof of address (such as a recent utility bill, bank statement, credit card bill etc). Overseas students must provide the appropriate visa documentation under UK Border Agency 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: Stephen Avery Job title: Chief Financial Officer Phone number: 01784 443016 Email: Stephen.Avery@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.	