Anti Money Laundering (AML) and Criminal Finances Act (CFA) Policy

Document owner: Deputy Director Financial Control
Date Approved by Audit and Risk Committee: 8 March 2018
Document updated: 21 February 2018
Reviewed by QMSE: 27 February 2018
Reviewed by Audit and Risk Committee: 8 March 2018
Recommended by Finance and Investment Committee: 13 March 2018
Approved by Council: 13 April 2018
Number of Years to Next Review: 3 Years –April 2021

Contents

Part 1: Anti Money Laundering

Page

Part 2 Criminal Finances Act

1. Introduction

Queen Mary University of London (QMUL) is committed to observing the provisions of the Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017, the Proceeds of Crime Act 2002, Part 7 – Money Laundering Offences and the Terrorism Act 2000 (as amended by the Crime and Courts Act 2013 and the Serious Crime Act 2013) in all of its affairs, whether academic or business related. This policy aims to ensure that QMUL and all its employees comply with the legislation and that the highest standards of due diligence are applied in relation to 'know your customer' principles.

This policy sets out the procedure to be followed if money laundering is suspected and defines the responsibility of individual employees in the process.

QMUL has a zero tolerance policy towards Money Laundering and is committed to the highest level of openness, integrity and accountability, both in letter and spirit. The penalties for these offences are severe and can mean up to 14 years imprisonment and/or an unlimited fine for the employees and executives responsible. In addition, there would be significant reputational damage for QMUL.

Any breach of this policy will be considered a serious matter and is likely to result in disciplinary action up to, and including, dismissal.

In addition to the Anti Money Laundering Policy, the following policies are available on the QMUL intranet:

- Financial Regulations
- Scheme of Delegation of Financial Authority
- Anti Bribery and Corruption
- Standards of Business Conduct
- Public Interest Disclosure (Whistle-blowing)
- Fraud and Corruption Policy and Response Plan

2. What is Money Laundering?

The introduction of the Proceeds of Crime Act 2002 and the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 has broadened the definition of money laundering and has widened the range of activities controlled by the statutory framework.

Money laundering covers a wide variety of crimes, it can include anything from which individuals or companies derive a pecuniary benefit, directly or indirectly, and can include many crimes that are not initially thought of as connected with money laundering. There is a risk where there are large volumes of cash transactions and where customer identification is not always easy, for example, cash received for overseas students.

Money laundering is the process by which criminally obtained money or other assets (criminal property) are exchanged for 'clean' money or other assets with no obvious link to their criminal

origins. Criminal property may take any form, including money or money's worth, securities, tangible property and intangible property. It also covers money, however come by, which is used to fund terrorism.

Money laundering offences include:

- Concealing, disguising, converting, transferring or removing criminal property from England and Wales (Section 327 of the Proceeds of Crime Act 2002 (POCA))
- Arranging, or becoming concerned in an arrangement, which the person who knows, or suspects, or facilitates (by whatever means), the acquisition, retention, use or control of criminal property by or on behalf of another person (Section 328, POCA)
- Acquiring, using or having possession of criminal property (Section 329, POCA)
- Making a disclosure to a person which is likely to prejudice a money laundering investigation ("tipping off") (Section 333, POCA)
- Becoming concerned in an arrangement facilitating concealment, removal from the jurisdiction, transfer to nominees or any other retention or control of terrorist property (Section 18, Terrorist Act 2000)

3. QMUL Obligations

QMUL has a responsibility to:

- Appoint a Money Laundering Reporting Officer (MLRO) to receive, consider and report as appropriate, the disclosure of any suspicious activity reported by employees.
- Implement a procedure to enable the reporting of suspicious activity.
- Maintain customer identification procedures to 'know your customer', in relevant circumstances.
- Maintain adequate records of transactions.

4. Employee Obligations

Money laundering legislation applies to ALL QMUL employees. 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. If any individual suspects that money laundering activity is or has taken place or if any person becomes concerned about their involvement it must be disclosed as soon as possible to the MLRO.

Failure to do so may result in you being personally liable to prosecution. Guidance on how to raise any concerns is included in this policy document.

5. Fees Paid and Refunds Requested in Cash

Money laundering regulations apply to cash transactions in excess of 15,000 Euros (or the equivalent in Sterling or other currencies). The Proceeds of Crime Act 2002, Part 7 – Money Laundering Offences applies to all transactions, including any dealings QMUL has with agents or third parties, and can involve cheques, cash, bank transfers and property or equipment.

Examples include:

- Where a student pays fees exceeding £10,000 (or equivalent) by cash
- Where a student pays a fee for another student who is not present at the time
- A sponsor/third party not known to QMUL pays fees for students

QMUL should avoid accepting cash payments greater than £10,000 (including notes, coins or travellers cheques in any currency). This does not mean that cash transactions below this value will be valid and legal and professional scepticism is encouraged at all times. Any suspicions should be reported to the MLRO (see below) and any advice followed.

Separate rules apply to foreign students and passports and visas of overseas applicants must be rigorously checked, and the UK Border Agency needs to be notified if a student with a Student Visa discontinues their studies. Fees paid in advance by foreign students who have subsequently been refused a visa are only refundable providing appropriate documentary evidence is available to demonstrate the circumstances. Where appropriate, refunds should only be made to the person making the original payment or in the case of a transfer by payment to the new University.

Care should also be taken where refunds are requested and the payment has been made by credit card or bank transfer. In these cases, refunds should only be made by the same method back to the same account from which funds were received. In the event of an attempted payment by credit or debit card being rejected the reason should be checked prior to accepting an alternative card. If in any doubt about the identity of the person attempting to make a payment the transaction should not be accepted.

6. 'Know your Customer'

It is important that controls are in place to undertake customer due diligence i.e. steps to identify the student, customer or other party dealing with QMUL. Satisfactory evidence of identity must be obtained. Examples include:

- Passport and/or Visa
- Birth Certificate
- Correspondence with students at their home address

And for third parties:

- Letters or documents proving name, address and relationship

If an organisation is not known to the University:

- Look for letter headed documents
- Check that invoices show a company's registered office and VAT number
- Check websites, for example, www.companies-house.gov.uk.
- Request a credit check
- Aim to meet or contact key sponsors if you feel appropriate to verify validity of contact

Cheques drawn on an unexpected or unusual source should always be verified with regard to validity of the source.

A guidance note on possible signs of money laundering is included at Appendix 2.

7. The Money Laundering and Proceeds of Crime Reporting Officer (MLRO)

The Director of Finance is the officer nominated to receive disclosures in respect of suspected transactions or activity within QMUL. Contact details can be found on the Intranet.

8. Disclosure Procedure to be followed by Individuals

Where you know or suspect that money laundering activity is taking or has taken place, or you become concerned that your involvement in a transaction may amount to a breach of the regulations, you must disclose this immediately to your line manager. If in consultation with your line manager reasonable suspicion is confirmed a disclosure report must be made to the MLRO. This disclosure should be made on the form shown at Appendix 3, which should be printed off and completed the same day the information came to your attention. If you do not do this, you may be personally liable to prosecution under the regulations.

Your report should include as much detail as possible including:

- Full details of the people and/or companies involved including yourself and other members of staff if relevant.
- Full details of the 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 you are 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 that may help to facilitate any report to the National Crime Agency (which replaced the Serious Organised Crime Agency).

Once you have reported your suspicions to the MLRO you must follow any instructions given to you. You must not make any further enquiries unless instructed to do so by the MLRO. At no time and under no circumstances should you voice any suspicions to the person(s) you suspect of money laundering, nor should you discuss this matter with any colleagues.

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 you may be committing a criminal offence. The penalty for tipping off is 5 years imprisonment and/or an unlimited fine.

9. Action and Disclosure by the MLRO

On receipt of a disclosure report the MLRO will:

- Note the date of receipt and acknowledge receipt of it.
- Assess and advise the individuals concerned when a response can be expected.
- Consider the report and any other relevant information, undertaking further enquiries if necessary to decide if a report should be made to the NCA.

Once the MLRO has evaluated the case, a timely determination will be made as to whether:

- There is actual or suspected money laundering taking place.
- There are reasonable grounds to know or suspect that is the case.
- Consent is required from NCA for a particular transaction to proceed.

Where the MLRO concludes that the case should be disclosed to NCA this needs to be done:

- In a timely manner.
- In the prescribed manner on a standard report format provided by NCA.

Where the MLRO concludes that there are no reasonable grounds to suspect money laundering then consent will be given for transactions to proceed and the disclosure report will be marked accordingly.

10. Record Keeping Requirements

By keeping comprehensive records QMUL will be able to show that we have complied with the Money Laundering Regulations. This is crucial if there is a subsequent investigation into one of our customers/students or transactions.

The types of record kept may include:

- Daily records of transactions
- Receipts
- Cheques
- Paying-in books
- Customer correspondence
- Student identification evidence

Records may be kept in any of the following formats:

- Originals
- Photocopies
- Microfiche
- Scanned
- Computerised or Electronic

Records must be kept for five years beginning on either:

- The date a business relationship ends
- The date a transaction is completed

In practice finance departments will routinely create and retain records in the course of normal business for six years. The Director of Finance will retain any disclosure reports and any associated relevant documents in a confidential file for a minimum of five years.

11. Conclusion

Instances of suspected money laundering are likely to be rare given the nature of services provided by QMUL. However, the increased tuition fees from 2012 may have an impact on cash transactions, therefore, we must be aware of the legislative requirements, as failure to comply would have serious implications for both QMUL and individuals concerned.
If you have any suspicions or concerns regarding possible money laundering please consult your line manager or the MLRO about your concerns.

Part 2 - Criminal Finances Act (CFA)

12. An introduction to criminal tax evasion

The Criminal Finances Act 2017 (CFA 2017) came into effect from 30th September 2017. Part 3 of the CFA 2017 introduces a new Corporate Criminal Offence (CCO) of failure to prevent the facilitation of tax evasion.

Whilst it has always been a criminal offence to evade tax, and for anyone to help someone else evade tax, the new Act means that if a person 'associated' to the university, anywhere in the world - is found to have assisted a third-party in evading tax in the course of their duties, then the university itself could be deemed to have committed a corporate offence.

The scope of 'Associated Persons' is widely drafted and, whilst it includes the university's officers, it also includes employees, workers, agents, sub-contractors and other people/organisations that provide services for, or on behalf of, the university. The new CCO relates to situations where the university fails to prevent 'Associated Persons' from assisting in the evasion of tax by another party.

13. The Criminal Finances Act 2017 (CFA 2017)

The university operates to the highest legal and ethical standards and will not tolerate acts of criminal facilitation of tax evasion by its associates anywhere in the world. The purpose of this policy is to set out the responsibilities of the university and of those working for it, whether as an officer, employee, worker, subcontractor, agent or in any other capacity.

The Criminal Finances Act 2017 has parallels with the UK Bribery Act and this policy should be read in conjunction with the university's anti-bribery and corruption policy and related governance documents.

It is a criminal offence for anyone to evade paying tax of any kind, and also to help anyone to do so. Any individual found to be guilty of this could be subject to criminal proceedings under existing legislation. However, under the CFA 2017 in the event of there being both:

- Criminal tax evasion by either a UK or overseas taxpayer (as an individual or an entity) under existing law, and,
- Criminal facilitation of this offence by an 'associated person' of the university

then the university will ***automatically be charged*** with the corporate offence of failing to prevent its representatives from committing the criminal act of facilitation ***unless*** it can demonstrate that it had 'adequate' or 'reasonable procedures' in place to prevent that facilitation. If found guilty, the typical consequences for the university could be an unlimited fine, reputational damage and the potential disbarment from public/governmental contracts.

14. Examples of facilitating tax evasion in a university context

The following are common university risks that could be expected to feature in a typical risk assessment document and/or risk register:

i. Making a payment overseas e.g. to an overseas agent in the knowledge that the agent intends to use the method of payment to evade tax. Typically, this could apply where a payment is made into a bank account which is not in the name of the agent or their company but in the name of a different individual or company, or to a jurisdiction where the individual does not live or work.

ii. Categorisation of a payment to an individual - who should be deemed an employee or treated as such under IR35 - as self-employed knowing that the individual will use the gross payment to evade tax.

iii. Assisting an academic to facilitate his/her personal use of department research accounts (or 'EDA') or the backdating of a waiver, resulting in a loss of income tax to HMRC.

iv. Making a royalty payment e.g. to an overseas academic/former academic in the knowledge that the academic intends to use the method of payment to evade tax. Again, this could be where a payment is made into a bank account which is not in the name of the academic but in the name of a different individual or company, or to a jurisdiction where the individual does not live or work.

v. Employee colludes with another university/third-party to mis-describe services as outside the scope, pass through or grant funding rather than a taxable supply of research services where VAT cannot be recovered.

vi. Employee agrees to mis-describe services provided to a third-party in order to facilitate a VAT reclaim by them.

vii. Employee agrees to mis-describe goods being exported so that a lower rate of Customs duty becomes payable on import by customer.

viii. Employee accepts request to pay one entity knowing that the goods/services have been provided by another entity and that the purpose of the change is to evade tax.

ix. Employee allows a payment for goods/services to be described as a donation so that the donor can claim tax relief.

x. Employee authorises a VAT invoice from a supplier knowing that they are not VAT registered.

xi. Employee authorises an expense claim with photocopied receipts knowing that the claimant will use the original receipts to support a tax reclaim.

xii. Employee agrees to mis-description of an income stream to take the payment outside a with-holding tax obligation.

xiii. Employee buys goods for personal use through a university account and issues a certificate for charitable relief.

xiv. Academics not employed by the university perform work in return for a payment in kind e.g. travel to a conference or use of facilities, knowing that no tax will be paid on the payment.

xv. Overseas agents mis-describe services to facilitate the evasion of local indirect taxes.

xvi. Using a third-party to pay in-country workers on the university's behalf, where you know that there is a withholding obligation, and that the third-party will not comply with that obligation.

HMRC has provided further generic examples of the facilitation of tax evasion and these can be found on HMRC website.

15. Responsibilities of university staff and Associated Persons

Staff and associates should abide at all times by university policies - including this CFA 2017 policy, the anti-bribery and corruption policy and related governance documents. Failure to comply with these policies and the obligations detailed in this policy may result in disciplinary action for staff (up to and including dismissal) and termination of contract for associated persons.
Should staff and associates become concerned that a fellow employee or associate is facilitating tax evasion by a third-party then they should immediately alert their manager or use the university whistle-blowing procedure.

16. Key Roles - The Criminal Finances Act 2017, including training

The university has made the appropriate appointments in relation to CFA 2017. The key officer will be responsible for questions, information, training and tax evasion reports in relation to CFA 2017. The university will provide relevant members of staff with training on the key aspects of CFA 2017, as set out in this policy. This training will be undertaken at a suitable frequency.

17. Risk Assessment - CFA & AML

Whilst the university has initiated a risk assessment in relation to the CFA - which will consider the relevant controls, processes and procedures - the risk assessment will form part of the wider work required for AML. This work is intended to ensure that all appropriate steps are taken to prevent facilitation of tax evasion.

A register of possible risks related to the facilitation of tax evasion by staff and/or associates will be prepared and maintained; the register will also list the controls to mitigate those risks and actions required to improve the controls. This register will be periodically reviewed and updated.

Appendix 1 - Risks to which Universities may be exposed

Courtesy of British Universities Finance Directors Group

The 2017 regulations place continuing emphasis on a risk-based approach to countering money laundering and terrorist financing. In practical terms this means identifying the risks facing the university, assessing the likely impact of these risks and putting in place procedures which will mitigate the risks.

Particular care needs to be focused on:

- Payments in cash
- Applicants from high risk countries
- Request for refunds
- Overpayments
- Failure to take up places
- Agents who do not fit in with normal procedures relating to deposits and tuition fees
- Identity fraud

Appendix 2 – Possible signs of money laundering

The following are types of risk factors which may, either alone or collectively, suggest the possibility of money laundering activity:

- A new customer, business partner or sponsor not known to QMUL
- A secretive person or business e.g. that refuses to provide requested information without a reasonable explanation or adequate documentation
- Attempted payment of any substantial sum in cash (over £10,000)
- Concerns about the honesty, integrity, identity or location of the people involved

- Involvement of an unconnected third party without a logical reason or explanation
- Overpayments for no apparent reason
- Absence of any legitimate source for the funds received
- Significant changes in the size, nature, frequency of transactions with a customer that is without reasonable explanation
- Cancellation, reversal or requests for refunds of earlier transactions
- Requests for account details outside the normal course of business
- A history of poor business records, controls or inconsistent dealing

Any other facts which tend to suggest that something unusual is happening and give reasonable suspicion about the motives of individuals.

If in doubt a Suspected Money Laundering form should be completed and returned to the Money Laundering Reporting Officer (MLRO).

Appendix 3 - Suspected Money Laundering – Report to the MLRO

From:_____School/Department:_____

Contact Details: E-mail:_____Phone:_____

DETAILS OF SUSPECTED OFFENCE

Name(s) and Address(es) of person(s) involved, including relationship with QMUL:

Nature, value and timing of activity involved:

Nature of suspicions regarding such activity:

Provide details of any investigation 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:_____

Appendix 4 - MLRO REPORT (to be completed by the MLRO)

Date Report Received:_____

Date Receipt of Report acknowledged:_____

CONSIDERATION OF DISCLOSURE

Further action required:

Are there reasonable grounds for suspicion requiring a report to be made to National Crime Agency (NCA):

If YES: Confirm date of report to NCA:_____

- Details on how to report can be found here:

http://www.nationalcrimeagency.gov.uk

- Via the online system:

  https://www.ukciu.gov.uk/(4dwdsb55ckchty55xezgys45)/saronline.aspx
- Address (if reporting by post):

  National Crime Agency Units 1 - 6 Citadel Place, Tinworth Street, London SE11 5EF

- Any further details:

- Is consent required from NCA to any on-going transactions?
- If YES: confirm details and instructions:

- Date consent received:_____
- Date consent given to staff:_____

If NO: Confirm reason for non-disclosure:

- Date consent given to staff:_____

Signed:_____Date:_____