UNIVERSITY OF WESTMINSTER

Anti-Money Laundering Policy 2025
(Proceeds of Crime)

Document owner: Director of Finance and Commercial Services
Document updated: 16 December 2024
Date Approved by University Executive Board: 7 January 2025
Approved by Audit Committee: 21 January 2025
Date Approved by Court: 12 March 2025
Number of Years to Next Review: 3 Years – February 2028

Contents

Part 1: Anti Money Laundering

1. Introduction

The University of Westminster (UoW) is committed to observing the provisions of the Money Laundering and Terrorist Financing (Amendment) Regulations 2023, 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 the University 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.

The University 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 the University.

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 UOW intranet:

- Financial Regulations
- Anti-Bribery and Corruption
- Public Interest Disclosure (Whistle-blowing)

2. What is Money Laundering?

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 or transferring criminal property or removing it 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. University Obligations

The University's approach to mitigating money laundering risk is based on the following key principles and has procedures in place to meet each of these:

- Appoint a Money Laundering Nominated Officer (MLNO) 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.
- Obtain satisfactory evidence of the identity of the customer/third party with whom the University deals/ or has a business relationship with (through Know Your Customer and Customer Due Diligence checks (see section 6). The extent of due diligence required will be guided by the anti-money laundering risk assessment. The higher the risk the greater the due diligence required.
- Retain evidence of the customer/ third party's identity and transactions made with them, maintaining adequate records of transactions for six years.
- Providing appropriate training to all relevant members of staff who are responsible for dealing with any transactions with university clients and or third parties. This is to ensure staff are aware of university procedures which guard against money laundering and the legal requirements relating to this. The University will keep records of all training undertaken.

4. Employee Obligations

Money laundering legislation applies to ALL University 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 MLNO.

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

The Proceeds of Crime Act 2002, Part 7 – Money Laundering Offences applies to all transactions, including any dealings the University has with agents or third parties, and can involve cheques, cash, bank transfers and property or equipment.

Examples include:

- Where a student pays fees 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 the University pays fees for students.

Separate rules apply to foreign students and passports and visas of overseas applicants must be rigorously checked, and the UK Visas and Immigration 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'

The University has established a Know-Your-Client (KYC) policy to ensure that the identities of all new and existing clients are ascertained and verified to a reasonable level of certainty. These checks include:

Ascertaining and verifying the identity of the customer/student, or third party – the University should be satisfied of the identity of the customer, or other third party with whom it is intending to engage in a business relationship; that is knowing who they are, confirming their identity is valid and verifying this by obtaining documents or other information from sources which are independent and reliable.

Ascertaining and verifying the identity of the beneficial owners of a business, if there are any, so we know the ultimate owners of the business or controllers of the business.

Information on the purpose and intended nature of the business relationship i.e. knowing what the University is going to do with/for them and why.

Identities will be verified either online or face-to face or by a combination of both.

The following documentation may be presented by the individual:

In person

- Either a passport, driver's license, or government issued document featuring a matching photograph of the individual, and a full name and date of birth matching those provided.
- An original recent utility bill, or government issued document with the same address matching those provided by the individual.

Not in person

As **in person** but additionally:

Any government issued document that provides the date of birth, NI or Tax number or other such government identifier.

Other forms of identity confirmation, such as evidence of a long standing relationship with the client, or a letter of assurance from independent and reliable persons or organisations, who have dealt with the client for some time, may also provide a reasonable level of certainty.

Only recognised online identity verification agencies, which use data from multiple sources over a period of time, will be used (such as CreditSafe and Companies House). These commercial agencies must have processes that allow the enquirer to capture and store the information they use to check and verify an identity.

If the University fails to verify the identity of a client with reasonable certainty it will not establish a business relationship or proceed with the transaction. If a potential or existing client either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, the University shall refuse to commence a business relationship or proceed with the transaction requested.

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

7. Reporting

7.1 Internal reporting

It is best practice for universities to appoint a nominated officer or Money Laundering Nominated Officer (MLNO) to be aware of any suspicious activity in the business that might be linked to money laundering or terrorist financing and if necessary report it through channels described below. The Director of Finance is the officer nominated to receive disclosures in respect of suspected transactions or activity within the University. Contact details can be found on the Intranet.

7.2 Disclosure Procedure to be followed by Individuals

Where a member of staff knows or suspects that money laundering activity is taking or has taken place or becomes concerned that their involvement in a transaction may amount to a breach of the regulations, and confirmed, wherever possible, this should not be discussed with any individual other than the MLNO and a disclosure report must be made. This disclosure should be made on the form shown at Appendix 3, which should be completed the same day the information came to their attention and emailed to the MLNO. Otherwise, they may be personally liable to prosecution under the regulations.

The referrer must not record their suspicion or record the matter on any system or document other than the disclosure report. The report should include as much detail as possible including:

- Full available details of the people and/or companies involved including themselves 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 they 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 MLNO judge the case for knowledge or suspicion of money laundering that may help to facilitate any report to the relevant authorities (National Crime Agency).

Once this suspicion has been reported to the MLNO any instructions given by the MLNO must be followed. Further enquiries must not be made unless instructed to do so by the MLNO. At no time and under no circumstances should you voice any suspicions to the person(s) suspected of money laundering, nor should this matter be discussed with any colleagues.

If appropriate the MLNO will refer the case to the relevant authorities (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 this may be committing a criminal offence. The penalty for tipping off is 5 years imprisonment and/or an unlimited fine.

7.3 External reporting- Action and Disclosure by the MLNO

On receipt of a disclosure report the MLNO 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 MLNO 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 MLNO 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 MLNO 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.

8. Monitoring - Record Keeping Requirements

To enable monitoring to be conducted and compliance with this policy evidenced, the University will retain all anti-money laundering and counter-terrorist finance records securely for a period of five years. This is crucial if there is a subsequent investigation into one of the University's customers/ students or transactions. By keeping comprehensive records, the University will be able to show that we have complied with the Money Laundering Regulations.

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.

9 Training

All employees are required to complete mandatory eLearning training that explains The Money Laundering and Terrorist Financing (Amendment) Regulations 2023, The Proceeds of Crime Act 2002 and section 18 and 21A Terrorism Act 2000 and how these affect their customers, firms and their employees as part of their induction process. All staff undertaking a finance function will receive refresher anti- money laundering and counter-terrorist training at least every 2 years or when the policy is revised. The training will include the applicable law, the operation of the anti-money laundering policy and how to identify and deal with transactions that may involve money laundering. A record of the course events will be maintained as evidence of this.

10 Conclusion

Instances of suspected money laundering are likely to be rare given the nature of services provided by the University. All employees are trained on their responsibilities in relation to money laundering legislation and are aware of how to identify and deal with transactions that may involve money laundering. If you have any suspicions or concerns regarding possible money laundering, please consult your line manager or the MLNO about your concerns.

Part 2: Criminal Finances Act

11 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.

12 The Criminal Finances Act 2017 (CFA2017)

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:

a. Criminal tax evasion by either a UK or overseas taxpayer (as an individual or an entity) under existing law, and,

b. 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.

13 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.

14 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.

15 Risk Assessment – CFA & AML

Because the offences are strict liability, the management need not have participated in, known about, or even suspected that their business's associated person was engaged in facilitating tax evasion. The mere fact of that facilitation will be sufficient to impute the business with criminal liability and it is therefore important for the University to demonstrate that it has in place "reasonable'' prevention procedures.

The University has initiated a risk assessment in relation to CFA to consider the relevant controls, processes and procedures in place to prevent the facilitation of tax evasion by staff and/or associates - the risk assessment forms 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.

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.

Appendices

Appendix 1 - Risks to which Universities may be exposed

Courtesy of British Universities Finance Directors Group

The 2007 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 – Money laundering signs and examples

Even though it is not possible to give a definitive list of ways to spot 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 the University.
- A secretive person or business e.g. that refuses to provide requested information without a reasonable explanation or adequate documentation
- Payment of any substantial sum in cash to the University
- 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 and requests to pay the difference back to a third party
- 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
- Receipt of a payment for which the University has not issued an invoice
- A receipt of fees from an unconnected third party (i.e. not a student, family member or sponsor)
- A customer from a country known to carry a high level of risk (such as a sanctioned country, or country with known high levels of financial fraud or corruption)

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 Nominated Officer (MLNO), (see Appendix 3).

Examples of how suspicion of money laundering may arise as part of their responsibilities

Example 1

A member of staff collects payments from international students. The member of staff establishes that payment for a student is being made by an unconnected/unknown third party. The staff member should report a suspicion by following the procedure outlined in sections 7.1 and 7.2.

Example 2

A staff member is made aware of a large or unexplained overpayment from or on behalf of an international student and a request for an overpayment be paid to a third party. The member of staff should report suspicion following the procedure in sections 7.1 and 7.2. Failure to report the suspicion or to act could be deemed as committing a money laundering offence. All refunds should be made to the original payee using the same payment method used to make the original payment. Where a staff member has any concerns or suspicion in respect of an overpayment and its legitimacy this must be reported and no further action taken (Appendix 3).

Appendix 3 - Suspected Money Laundering – Report to the MLNO *(policy reference section 7.2)*

From:_____School/Department:_____

Contact Details: E-mail:_____Phone:_____

DETAILS OF SUSPECTED OFFENCE

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

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 - MLNO REPORT *(to be completed by the MLNO, policy reference section 7.3)*

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, PO Box 8000, London, SE11 5EN Tel: 020 7238 8282, Fax: 020 7238 8286
- □ 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:_____