ANTI MONEY LAUNDERING AND COUNTER TERRORIST FINANCING POLICY

May 2023

Contents

Document title	
Anti Money Laundering and Counter Terrorist Financing Policy	
Document author and department	
Financial Controller	
Approving body	
Audit and Quality Committee	
Date of approval	
22.05.2023 (operational update March 2024)	
Review date	
May 2025	
Edition no.	
6	
ID Code	
143	
Date of effect	
22.05.2023	
For a) public access online internet or b) staff only intranet?	Both
External queries relating to the document to be referred in the first instance to the Corporate Governance team: email corporate-governance@port.ac.uk If you need this document in an alternative format, please email corporate.communications@port.ac.uk	

The latest version of this document is always to be found at:

http://policies.docstore.port.ac.uk/policy-143.pdf

Summary

What is this document about?

- This policy explains the steps the University and its UK based subsidiaries are taking to prevent and deter money laundering and terrorist financing, and it summarises the responsibilities of all persons associated with the University and its UK based subsidiaries in preventing and deterring these criminal activities.
- It details the appropriate persons and agencies to report suspected money laundering and terrorist financing to, and the steps to be followed in the event of money laundering and/or terrorist financing being suspected or detected.

Who is this for?

All staff but for those in particular who are involved in the decision to accept students or business on behalf of the University and its UK subsidiaries, staff who are involved with identifying students and other customers, and staff involved with the process of receiving funds or processing refunds.

How does the University check this is followed?

Through the Financial Controller team, in particular the Anti Money Laundering Compliance Manager, and internal auditors.

Who can you contact if you have any queries about this document?

The Anti Money Laundering Nominated Officer, which is the Chief Financial Officer (Financial Services).

Executive summary

In recent years, Universities have become unwilling participants at increased risk of money laundering by criminals that are creative in seeking out new opportunities.

Compared to banks, accountants and law firms that are heavily regulated, Universities have been seen as an easy target by criminals as they are largely unregulated with regards to money laundering and terrorist financing (MLTF).

Examples of MLTF activity that takes place within Universities (including Portsmouth) involve students becoming caught up in credit card scams (money-mules), payments from students with links to Politically Exposed People (PEP's) or criminals attempting to pay for family education using illicit funds.

The University of Portsmouth has taken significant steps in reducing its MLTF risk by removing the option for students to pay in cash, and also by preventing students from paying directly over the branch counter at our main clearing bank, Lloyds.

The AMLTF Policy summarises the AML offences and sets out the University's obligations, responses and the procedures to be followed to ensure AMLTF compliance.

Introduction

Policy Aims

1) The University is committed to ensuring the highest standards of probity in all of its financial dealings. It will therefore ensure that it has in place proper, robust financial controls so that it can protect its funds and ensure continuing public trust and confidence in it. Some of those controls are intended to ensure that the University complies in full with its obligations not to engage (or otherwise be implicated in) money laundering or terrorist financing. This policy sets out those obligations, the University's response and the procedures to be followed to ensure compliance. This policy applies to the University together with its UK based subsidiaries. Any overseas subsidiaries will refer to the law of their local jurisdiction.

Implementation

2) The Financial Controller is directly responsible to the Audit and Quality Committee for the implementation of this policy and will ensure:

    i) regular assessments of the University's money laundering and terrorist finance risks are conducted and relied on to ensure the effectiveness of this policy;
    ii) appropriate due diligence is conducted, as a result of which risks relating to individual transactions are assessed, mitigated and kept under review;
    iii) reporting by exception to the Chief Financial Officer, including raising any immediate issues as necessary;
    iv) anti-money laundering and counter-terrorist finance training is delivered within the University, including training on this policy; and
    v) this policy is kept under review and up-dated as and when necessary and levels of compliance are monitored.

3) The Money Laundering Reporting Officer (MLRO) is responsible for oversight of the University's Anti-Money Laundering and Counter Terrorist Financing (AMLTF) systems and controls, and for receiving internal suspicious transaction reports, where there is knowledge or suspicion of money laundering or terrorist financing. For the purposes of this policy, the MLRO is the Chief Financial Officer (Financial Services).

4) All staff are responsible for ensuring compliance with the Anti Money Laundering and Counter Terrorist Financing Policy, however specific responsibility rests with those staff:

    a) that are engaged in financial transactions particularly the allocation of funds to student accounts and refunds;
    b) that are involved with the decision to accept students for and on behalf of the University;
    c) that are involved with the decision to accept other business for or on behalf of the University;

d) that are involved in the acceptance of identification and address verification of students for and of behalf of the University;
e) that are involved in the acceptance of identification and address verification of businesses for and on behalf of the University.

5) Any member of staff that fails to comply with this policy will be subject to disciplinary action under the University's Disciplinary Procedures and may also expose themselves to the risk of committing a criminal offence. Training and support to relevant staff will be given annually by the Anti-Money Laundering Compliance Manager, to ensure compliance with this policy.

What is Money Laundering?

6) Money laundering is the process by which the proceeds of crime are legitimised and sanitised in order to disguise their illicit origins. 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. Schemes are evolving and getting more sophisticated all the time.

7) The law concerning money laundering is complex. The UK anti-money laundering requirements are set out in the Proceeds of Crime Act 2002 (POCA), and the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017);

8) There are three main types of offences:

i) the principal money laundering offences (under the Proceeds of Crime Act 2002);
ii) tipping off (prejudicing investigations offence also under the Proceeds of Crime Act 2002);
iii) failing to comply (with the administrative requirements of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017).

Money Laundering Warning Signs or Red Flags

9) Payments (or prospective payments) made to or requested from the University can generate a suspicion of money laundering for a number of different reasons. For example, where a payment to the University is made by a third party with no logical connection between the third party and the student (other examples of suspicious activity can be found in Appendix 1).

Principal Money Laundering Offences

10) Criminal property is any property (such as cash, bank accounts, or physical assets) that has been derived from criminal conduct.

11) Under the Proceeds of Crime Act 2002, it is a crime to:

a. "conceal, disguise, convert, or transfer criminal property…"

b. "enter into an arrangement that… makes it easier for another person to acquire, retain, use or control criminal property"

c. "acquire, use or "acquire, use or possess criminal property…"

12) University Staff can unknowingly commit these offences when handling or dealing with payments to the University. For example, where staff of the University make a repayment to a student they risk committing offences a and b. Where staff of the University receive funds from a stolen credit card and allocate this to a debtors account in settlement of fees owed, they risk committing offence c.

13) In both of these cases, staff will have a defence if they make an authorised disclosure to the Financial Controller as soon as they become aware.

Defences to the Principal Money Laundering Offences

14) Where the University suspects money laundering, it must immediately suspend activity on the payers account and make a "Suspicious Activity Report (SAR)" to the National Crime Agency (NCA).

15) As part of the SAR, the University will always seek a "Defence against money laundering (DAML)". Once a DAML has been granted (or after 7 days when permission can be assumed to be granted) the funds may then be returned to the payer, or the payment accepted without further recourse or risk of prosecution.

The Offence of Prejudicing Investigations / Tipping-Off

16) The purpose of making an authorised disclosure to the National Crime Agency is to allow it to investigate suspected money laundering so it can decide whether to refuse consent to the transaction.

17) 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 the Proceeds of Crime Act 2002 provides that it is a crime to make a disclosure which is likely to prejudice the money laundering investigation.

18) University staff can commit this offence if they tell a person an authorised disclosure has been made in their case, for example when a student calls in to enquire why the payment they made is not showing on their account.

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017

19) These regulations are aimed at protecting the gateway into the financial system. They apply to a range of businesses all of which stand at that gateway. They require these businesses to conduct money laundering risk assessments and to establish policies and procedures to manage those risks. Businesses to which the regulations apply are specifically required to conduct due diligence of new customers, a process known as "Know your Customer" or "KYC".

20) Whilst the University is not covered by the regulations in its work as a provider of education, some of its activities are, for example, Technopole Enterprises Ltd. TEPL provide registered offices, business addresses and correspondence addresses for some of its customers and are therefore required to be regulated as a Company Service Provider.

The Principal Terrorist Finance Offences

21) 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.

22) Payments or prospective payments made to or asked of the University 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 (FATF [3] Blacklist).

23) It is an offence when a person believes or suspects Terrorist Finance and does not report it.

Defences to the Principal Terrorist Finance Offences

24) 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.

Our Procedures

Overview

25) The University will:

i) conduct an annual risk assessment to identify and assess areas of risk money laundering and terrorist financing particular to the University;
ii) implement controls proportionate to the risks identified;
iii) establish and maintain procedures to conduct due diligence on funds received;
iv) review policies and procedures annually and carry out on-going monitoring of compliance with them;
v) appoint a MLRO to be responsible for reporting any suspicious transactions to the National Crime Agency;
vi) provide training to all relevant members of staff, including temporary staff, on joining the University, and provide annual refresher training;
vii) maintain and retain full records of work done pursuant to this policy; and

viii) report to the Audit and Quality Committee on all aspects of this policy, including its implementation.

Transaction Due Diligence

26) Due diligence is the process by which the University 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 University 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.

27) In practical terms this means:

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

28) Source of funds refers to where the funds in question are received from. The most common example of a source of funds is a bank account. Source of wealth refers to how the person making the payment came to have the funds in question. An example of a source of wealth is savings from employment.

29) Practical application guidance will support our procedures and should be read alongside this Policy.

Transaction Risk Assessment

30) Having completed its due diligence exercise, the University will assess the money laundering and terrorist finance risk associated with the proposed transaction.

31) Due to the number of transactions processed by the University in 2021/22 at approximately 5,000 per month, the University has adopted a risk-based approach to manage this task. Using the risk scoring matrix found at Appendix 2, a score will be calculated for each transaction and a decision made as to the risk of Anti Money Laundering or Terrorist Financing.

32) Where the transaction is considered suspicious or the member of staff dealing with the case otherwise considers there is a suspicion of money laundering or terrorist finance, they must report the case as soon as practicable to the Financial Controller, by emailing Link to email address for Financial Controller.

33) The Financial Controller will consider the report and will decide:

i) Whether or not to accept or to make the proposed payment;

ii) Whether or not to make an authorised disclosure to the National Crime Agency;
iii) Whether or not to make a disclosure under the Terrorism Act 2000; and
iv) Whether this has implications for the delivery of the University's Prevent duty and should be reported to the University's Prevent lead staff member.

34) The Financial Controller will record in writing the reasons for their decision and retain that record centrally, to be shared with the Chief Financial Officer on a quarterly basis. Information that an authorised disclosure has been made must never be kept on the file relating to the person concerned.

35) Risk assessments relating to individuals and authorised disclosures are to be kept strictly confidential and should not be discussed within the Finance Department except on a strict need-to-know basis. No member of staff may reveal to any person outside the Finance 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.

Monitoring

36) The Financial Controller will devise and implement arrangements to ensure that compliance with this policy is kept under continuous review through regular file reviews, including reviews of due diligence and risk assessment, and reports and feedback from staff. Internal audit may be called upon to assist in monitoring effective implementation of this policy. These arrangements will be reviewed annually, and will be subject to periodic internal audit review.

37) To enable monitoring to be conducted and compliance with this policy to be evidenced, the University will retain all anti-money laundering and counter-terrorist finance records securely for a period of at least five years.

Training

38) On joining the University any relevant staff as identified in paragraph 4 will receive anti-money laundering training as part of their induction process and receive annual refresher anti-money laundering and counter-terrorist finance training.

39) The University's anti-money laundering and counter-terrorist financing training will include the applicable law, the operation and practical application of this policy and the circumstances in which suspicions might arise.

40) The University will make and retain for at least five years records of its anti-money laundering training.

Donations

41) To help prevent money laundering, universities should assess the levels of risk to which they are exposed and adopt appropriate anti-money laundering procedures. These might include:

i) due diligence checks on the donor, considering factors such as size of donation, source of funds and donor's location

ii) further verification checks when the donor is considered higher risk

iii) ensuring that staff know how to recognise the warning signs of possible money laundering

iv) robust methods for recording and documenting donations and grants

v) protocols for monitoring the effectiveness of the money laundering procedures

42) The University should take reasonable and appropriate steps to know who the donors are, particularly where significant sums are being donated or the circumstances of the donation give rise to notable risk. Good due diligence will help to:

i) assess any risks to the University that may arise from accepting a donation or certain types of donations
ii) ensure that it is appropriate for the University to accept money from the particular donor, whether that is an individual or organisation
iii) give reasonable assurance that the donation is not from any illegal or inappropriate source
iv) ensure that any conditions that may be attached are appropriate and can be accepted

The University needs to put effective processes in place to provide adequate assurances about the identity of donors, particularly substantial donors, taking steps to verify this where reasonable and it is necessary to do so (ie 'identify' and 'verify'). They should also have assurance on the provenance of funds and the conditions attached to them 'i.e. know what the donor's specific business is with the University' and ensure they know the rules of, and their responsibilities under, relevant legislation on substantial donors. This does not mean we have to question every donation. Nor must we know lots of personal and other details about every donor.

43) Some donors give relatively small amounts of money as a one-off donation, by cheque or bank transfer. We are not expected to know the identity or take steps to find out the identity of each small donor in these sorts of circumstances. This would not be reasonable or necessary.

Some individuals and organisations will donate regularly to the University and set up regular payments through direct debits. We will already have the name, address and details of those donors and their bank details to collect the money and if they wish to collect gift aid. Therefore, it is unlikely that we will need to take any further steps here. If the University is claiming Gift Aid, it is required to maintain a record of the donor's details (the name and postcode are the minimum requirements).

44) Other donors give significant grants to universities and the University may have a close working relationship with them. It is for significant donors like these that we are likely to need to carry out further due diligence and take steps to identify and verify the identity of the donor so we can assess any risks. For example, if you know that the donor you are familiar with is from a country or operates a business, perhaps outside of the UK, about which public concerns have been raised, then the University should take more steps to verify the provenance of the funds.

If there is a significant donor which is an organisation, the University 'should know what its business is' and be assured that the organisation is appropriate for the University to be involved or linked with. If a donor is a charity, its registration and details can be checked with the relevant charity regulator, for example in the case of England and Wales on the Register of Charities. If the donor is a company, its details can be checked on the Companies House website.

Sometimes risks can be identified by carrying out a check on the organisation's website or using

other internet search engines to look at other information written about it. However, care should be taken to assess how reliable the information is. For example, is the information repeating allegations others have made? Were they proven? How old is the information?

45) In accordance with our duties to act in the best interests of the University and maintain its integrity, we should consider carefully donations from sources that might be seen to compromise the University's reputation, independence and work. Key benefits of due diligence steps are:

i) ensuring we have a reasonable degree of confidence about the provenance of the donation and that there is no reason to believe it is suspicious
ii) exposing legal reasons why the University should not accept the donation (for example because the organisation is proscribed or there is a significant risk that the money comes from illegal sources) or operational reasons (for example the donor's activities or ethics may give rise to risks to the University).
iii) identifying if there are any requirements or conditions attached to the donation – sometimes the conditions may mean the University has to refuse the donation
iv) understanding the intentions of donors and any restrictions placed on the money received - a good relationship with donors which is open and transparent is essential for building trust and confidence and ensuring that the expectations and commitments of both parties are clear, being clear about this will also ensure that the University does not disappoint its donors where there are expectations, and could help with securing longer term funding

Appendix 1

Examples of Suspicious Activity

i) 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 University, or
   c) where a debt to the University is settled by various third parties making a string of small payments

ii) payments from third parties who are foreign public officials or who are politically exposed persons ("PEP");

iii) payments made in an unusual or complex way;

iv) donations which are conditional on particular individuals or organisations, who are unfamiliar to the University, being engaged to carry out work;

v) requests for refunds of advance payments, particularly where the University is asked to make the refund payment to someone other than the original payer;

vi) a series of small payments made from various credit cards with no apparent connection to the student and sometimes followed by chargeback demands;

vii) 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;

viii) prospective payers are obstructive, evasive or secretive when asked about their identity or the source of their funds or wealth;

ix) prospective payments from a potentially risky source or a high-risk jurisdiction;

x) the payer's ability to finance the payments required is not immediately apparent or the funding arrangements are otherwise unusual.

Appendix 2

Payment Transaction Risk Scoring Matrix

Risk Score	Nationality / Domicile	Remitter Relationship	Payment Method	Number of payment attempts	Transaction Value
1	United Kingdom	Student or Parent/Guardian/Sibling (with same name/evidenced relationship)	UK card or UK bank transfer or Third party provider who completes due diligence on payer (e.g. WUBS[1]/Flywire)	<3 - same payer details	Paying for no more than one year of study.
2	EU	Parent/Guardian/Sibling (different name/ no evidence of relationship)		3-10 - same payer details	
3		Other 'Relative'	International card payment		
5	Law Society High Risk AML Countries PEP[2]	Agent	Unknown third-party provider (For example Swoosh)		Paying for more than one year of study (but less than the full course)
6	FATF[3] Greylist		International bank transfer		
9	HMRC increased risk list	Unrelated third party			
10	FATF[3] Blacklist, HMRC high risk list	Unknown / Suspicious and/or multiple payers Identity of payer cannot be established	Cash	>3 different payer details	Paying for all years of study in advance
Score					

Appendix 2 (continued)

Payment Transaction Risk Scoring Matrix

Range	Risk	Action Required
0 – 8	Low	No additional checks required, payments may be processed and allocated to student account
9 – 29	Medium	Further checks are required to mitigate risks
30 – 44	High	Further checks are required to mitigate risks and Financial Controller officer sign off is required.
45 - 50	Very High	Refer to Financial Controller for further advice. Likely prepare SAR and DAML and return funds.

Key to Scoring Matrix Terms

[1] WUBS- Western Union Business Solutions

[2] PEP-Politically exposed person

[3] FATF-Financial Action Task Force (the global money laundering and terrorist financing watchdog)

Appendix 3

Summary of the Legislation

Section and Act	Offence	Punishment
Sections 15 to 18 Terrorism Act 2000	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).	up to fourteen years imprisonment
Sections 327, 328 and 329 Proceeds of Crime Act 2002	i) conceal, disguise, convert or transfer criminal property or to remove it from the United Kingdom; 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.	up to fourteen years imprisonment
Sections 330 Proceeds of Crime Act 2002	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 (s)he received the information.	up to five years imprisonment
Section 342 Proceeds of Crime Act 2002	To make a disclosure which is likely to prejudice the money laundering investigation.	up to five years imprisonment
Section 19 Terrorism Act 2000	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 their employer's procedures.	up to five years imprisonment
Section 39 Terrorism Act 2000	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.	up to five years imprisonment

University of Portsmouth
University House
Winston Churchill Avenue
Portsmouth PO1 2UP
United Kingdom

T: +44 (0)23 9284 3199

E: corporate-governance@port.ac.uk
W: www.port.ac.uk