Anti Money Laundering and Counter Terrorist Financing Policy			
Document type:	Policy		
Document number:	FIN-291	Version:	01
Department:	Finance and Procurement		
Approved by:	Executive Board	Date approved:	27/10/2025
Effective from:	01/11/2025	Review date:	31/10/2027
Publication:	SOAS website		
Related documents:	N/A		
Documents replaced:	N/A		
Note: All policies must be read in conjunction with all other SOAS policy, procedure and guidance documents. Printed copies of policies may not be the most up to date, therefore please refer to the policy pages on the SOAS external website or intranet for the latest version.			

1. Policy Aims

1.1. 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.

2. Implementation

2.1. The Chief Financial Officer is directly responsible to the Board for the implementation of this policy. As such, with the Board full support, he/she 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) anti-money laundering and counter-terrorist finance training is delivered within the University, including training on this policy; and

iv) this policy is kept under review and up-dated as and when necessary and levels of compliance are monitored.

2.2. Certain functions under this policy are to be undertaken by a Nominated Officer. For the purposes of this policy, the Nominated Officer is the Chief Financial Officer and, in their absence, their deputy.

2.3. This policy applies to all staff who are engaged in financial transactions for or on behalf of the University. Any failures to adhere to this policy may be dealt with under the University's disciplinary or poor performance policies, as appropriate. Note that any such failures also expose the individual concerned to the risk of committing a money laundering offence.

3. What is Money Laundering?

3.1. Money laundering is the process by which the proceeds of crime are sanitised in order to disguise their illicit origins and are legitimised. 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. Money laundering schemes typically involve three distinct stages:

i) placement – the process of getting criminal money into the financial system;

ii) layering – the process of moving the money within the financial system through layers of transactions; and

iii) integration – the process whereby the money is finally integrated into the economy, perhaps in the form of a payment for a legitimate service.

4. Money Laundering Warning Signs or Red Flags

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

i) large cash payments;

ii) multiple small cash payments to meet a single payment obligation;

iii) payments or prospective payments from third parties, particularly where

a. there is no logical connection between the third party and the student, or

b. where the third party is not otherwise known to the University, or

c. where a debt to the university is settled by various third parties making a string of small payments;

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

v) payments made in an unusual or complex way;

vi) unsolicited offers of short-term loans of large amounts, repayable by cheque or bank transfer, perhaps in a different currency and typically on the basis that the University is allowed to retain interest or otherwise retain a small sum;

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

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

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

x) the prospective payer wants to pay up-front a larger sum than is required or otherwise wants to make payment in advance of them being due;

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

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

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

5. Money Laundering - The Law

5.1. The law concerning money laundering is complex and is increasingly actively enforced. It can be broken down into three main types of offences:

i) the principal money laundering offences under the Proceeds of Crime Act 2002;

ii) the prejudicing investigations offence under the Proceeds of Crime Act 2002; and

iii) offences of failing to meet the standards required of certain regulated businesses, including offences of failing to disclose suspicions of money laundering and failing to comply with the administrative requirements of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.

The Principal Money Laundering Offences

5.2. These offences, contained in sections 327, 328 and 329 Proceeds of Crime Act 2002, apply to any property (e.g. cash, bank accounts, physical property, or assets) that constitutes a person's benefit from criminal conduct or any property that, directly or indirectly, represents such a benefit (in whole or partly) where the person concerned knows or suspects that it constitutes or represents such a benefit. Any property which meets this definition is called criminal property. It is a crime, punishable by up to fourteen years imprisonment, to:

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.

5.3. University staff can commit these offences when handling or dealing with payments to the University: if they make or arrange to make a repayment, they risk committing the first two offences, and if they accept a payment, they risk committing the third offence.

Defences

5.4. In all three cases, they will have a defence if they made a so-called *authorised disclosure* of the transaction either to the Nominated Officer or to National Crime Agency and the National Crime Agency does not refuse consent to it.

Failure to Disclose Offence

5.5. It is a crime, punishable by up to five years imprisonment, for a Nominated Officer who knows or suspects money laundering or who has reasonable grounds to know or suspect it, having received an authorised disclosure not to make an onward authorised disclosure to the National Crime Agency as soon as practicable after he/she received the information.

5.6. At paragraph **Error! Reference source not found.** below, this policy sets out how such disclosures are to be made.

The Offence of Prejudicing Investigations / Tipping-Off

5.7. The purpose of making an authorised disclosure to the National Crime Agency is to allow it to investigate the suspected money laundering so it can decide whether to refuse consent to the transaction. That investigation would be compromised if the person concerned (or indeed anyone else) were to be told that an authorised disclosure had been made. To prevent this happening section 342 Proceeds of Crime Act 2002 provides that it is a crime, punishable by up to five years imprisonment, to make a disclosure which is likely to prejudice the money laundering investigation. University staff can commit this offence if they tell a person an authorised disclosure has been made in their case. At paragraph **Error! Reference source not found.** below, this policy requires authorised disclosures to be kept strictly confidential.

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

5.8. 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". There are criminal sanctions, including terms of imprisonment of up to two years, for non-compliance. Whilst the University is not covered by the regulations in its work as a provider of education, the regulations provide a guide to the management of risk in handling money and due diligence is at the heart of the University's approach in this policy to managing risk.

5.9. To the extent that the University is regulated by the Financial Conduct Authority for part of its business, it must comply with Money Laundering Regulations (and a separate, more detailed policy sets out the university's approach here).

Terrorist Finance

The Principal Terrorist Finance Offences

5.10. 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.

5.11. 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.

5.12. Sections 15 to 18 Terrorism Act 2000 create offences, punishable by up to 14 years imprisonment, of:

i) raising, possessing or using funds for terrorist purposes;

ii) becoming involved in an arrangement to make funds available for the purposes of terrorism; and

iii) facilitating the laundering of terrorist money (by concealment, removal, transfer or in any other way).

5.13. These offences are also committed where the person concerned knows, intends or has reasonable cause to suspect that the funds concerned will be used for a terrorist purpose.

5.14. 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.

5.15. Section 19 Terrorism Act 2000 creates an offence, punishable by up to five years imprisonment, where a person receives information in the course of their employment that causes them to believe or suspect that another person has committed an offence under sections 15 to 18 of Terrorism Act 2000 and does not then report the matter either directly to the police or otherwise in accordance with their employer's procedures. This policy sets out those procedures at paragraph 32 below.

The Offence of Prejudicing Investigations

5.16. Section 39 Terrorism Act 2000 creates an offence, punishable by up to five years imprisonment, for a person who has made a disclosure under section 19 Terrorism Act 2000 to disclose to another person anything that is likely to prejudice the investigation resulting from that disclosure. At paragraph **Error! Reference source not found.** below, this policy requires disclosures under the Terrorism Act 2000 to be kept strictly confidential.

6. Our Procedures

Overview

6.1. 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 policies and 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 Nominated Officer 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; and

vii) maintain and retain full records of work done pursuant to this policy.

The University's Risk Assessment, Continuous Review and Accountability

6.2. At least once a year, and more frequently if there is a major change in circumstances, the Chief Financial Officer will:

i) conduct an assessment of money laundering and terrorist finance risk in the University's work;

ii) review and, if necessary, revise this policy in light of that risk assessment;

iii) review and, if necessary, revise the University's arrangements for ensuring compliance with this policy so that resources are targeted to the areas of greatest risk; and

iv) report to the Board on all aspects of this policy, including its implementation.

6.3. In order to facilitate the review and accountability functions, the Chief Financial Officer will ensure:

i) the availability of appropriate management information to permit effective oversight and challenge; and

ii) the maintenance and retention of full records of work done under this policy.

6.4. In conducting the assessment of money laundering and terrorist financing risk arising from the University's work and funding activity, the Chief Financial Officer/Bursar will have regard to the University's experiences and to any lessons learned in applying this policy. They will also take into account any guidance or assessments made by the UK government, law enforcement and regulators, including the Charity Commission, the Office for Students and the Financial Conduct Authority. They may also have regard to reports by non-governmental organisations and commercial due diligence providers.

Transaction Due Diligence

6.5. 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.

6.6. In practical terms this means:

i) identifying and verifying the identity of a payer or a payee, typically a student or a donor;

ii) where the payment is to come from or to be made by a third party on behalf of the student or donor, identifying and verifying the identity of that third party;

iii) identifying and verifying the source of funds from which any payment to the University will be made; and

iv) identifying and in some circumstances verifying the source of wealth from which the funds are derived.

6.7. 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.

Transaction Risk Assessment

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

6.9. Where the case falls into the category of case described in Annex 1 as suspicious or the member of staff dealing with the case otherwise considers there is a suspicion of money laundering or terrorist finance, he/she must report the case as soon as practicable, by email, to the Nominated Officer on a Form 1, which is to be found at Annex 2.

6.10. The Nominated Officer 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; and

iii) whether or not to make a disclosure under the Terrorism Act 2000.

6.11. The Nominated Officer will record in writing the reasons for their decision and retain that record centrally. Information that an authorised disclosure has been made must never be kept on the file relating to the person concerned.

6.12. 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

6.13. The Chief Financial Officer 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.

6.14. 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

6.15. On joining the University any staff whose duties will include undertaking a finance function will receive anti-money laundering training as part of their induction process.

6.16. All staff undertaking a finance function will receive annual refresher anti-money laundering and counter-terrorist finance training.

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

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

Annex 1 - Guidance on Identifying and Verifying Payments for Students and Third Parties

Purpose

To provide staff with a clear process for conducting due diligence when receiving payments from students, donors, or third parties on their behalf.

1. A. Steps for Student Payments

1.1. **Identify the Payer:**

- Confirm full legal name, student ID, and permanent address.
- Obtain and verify government-issued photo identification (passport, national ID, or driver's licence).

1.2. **Verify the Source of Funds:**

- Payments should ordinarily come directly from the student's bank account.
- Where this is not the case, ensure documentary evidence is provided (e.g., bank statement, scholarship award letter, sponsorship agreement).

1.3. **Check for Red Flags:**

- Large or unusual cash payments.
- Payments inconsistent with the student's profile.
- Requests for refunds to third-party accounts.

2. Steps for Third-Party Payments (Sponsors, Family, Employers, Donors)

2.1. **Identify the Third Party:**

- Obtain the individual's or organisation's full name, address, and relationship to the student.
- For organisations: request registration details and official documentation.

2.2. **Verify the Source of Funds:**

- Request supporting evidence of the third party's ability to provide funds (e.g., payslip, audited accounts, bank statement).

2.3. **Additional Caution for High-Risk Cases:**

- Payments from high-risk jurisdictions.
- Politically Exposed Persons (PEPs).
- Donations with unusual conditions attached.

3. C. Actions if Suspicious

If any of the above raise suspicion, complete Form 1 (Annex 2) and submit to the Nominated Officer immediately. Do not inform the payer or student.

Annex 2 – Suspicious Activity Report (Form 1)

CONFIDENTIAL – To be sent directly to the Nominated Officer

1. Reporter's Details	Name, Position, Department, Contact Information
2. Date of Report	[Insert date]
3. Transaction Details	Amount, Currency, Payment Method, Date of Payment, Account Details
4. Payer Details	Full Name, Address, Relationship to Student, Identification Provided
5. Student/Beneficiary Details	Full Name, Student ID, Course/Programme, Contact Information
6. Source of Funds (if known)	Bank name, account details, explanation provided
7. Suspicious Indicators	- Large/unusual cash payment - Multiple small payments - Third-party with no clear link - High-risk jurisdiction - Refund request to different account - PEP involvement - Other (please specify)
8. Description of Suspicion	[Free text – provide full details of why you believe this transaction may involve money laundering or terrorist financing]
9. Action Taken So Far	[e.g., payment held pending review]
10. Declaration	I believe the information above is accurate and submit this in compliance with the University's AML Policy.
Signature of Reporter	
Date	

To be completed by the Nominated Officer only	
Date Received	
Action taken	
Disclosure to NCA:	Yes / No
Reference number (if applicable):	