Anti-Money Laundering and Counter Terrorist Financing Policy

Swansea University
Prifysgol Abertawe

Owner	Chief Financial Officer
Version number	5.0
Date of approval	March 2026
Approved by	Audit, Assurance & Risk Committee
Effective date	March 2026
Date of next review	March 2028

1. Introduction

1.1 Policy Aims

The University is committed to ensuring the highest standards of probity in 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. 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. It aims to protect employees and University funds, whilst ensuring the continued public trust and confidence.

1.2 Scope

This Policy applies to all employees who engage in activities on behalf of the University and its subsidiary companies. As such, it applies to:

- Swansea University and subsidiary employees.
- All University and subsidiary income, payments, and requests to receive income or make payment in the UK and overseas.

1.3 Compliance

All University and subsidiary activity must be in accordance with this Anti-Money Laundering and Counter Terrorist Policy and other associated University policies.

Compliance is mandatory. Failure to do so may be dealt with under the University's conduct procedures and may also expose the individual concerned to the risk of committing a money laundering offence.

2. Nominated Officer and accountable persons

2.1 Nominated Officer

The Nominated Officer is the Chief Financial Officer (s.n.jones@swansea.ac.uk). All suspicions or concerns regarding money laundering or counter terrorist financing must be reported to the Nominated Officer without delay.

Where the Nominated Officer is absent, reports are to be made directly to their deputy, the Associate Director of Finance (n.s.owen@swansea.ac.uk).

The Nominated Officer is directly accountable to the Accountable Person.

2.2 Accountable Persons

The Vice Chancellor is directly accountable to Council for the implementation of this policy. As such, they will ensure:

- regular assessments of the University's money laundering and terrorist finance risks are conducted and relied on to ensure the effectiveness of this policy.
- appropriate due diligence is conducted, as a result of which risks relating to individual transactions are assessed, mitigated and kept under review.
- anti-money laundering and counter-terrorist finance training is delivered within the University; and
- this policy is kept under review and updated as and when necessary and levels of compliance are monitored.

All employees are accountable for their actions under this policy.

3. What is money laundering?

3.1 What is money laundering?

Money laundering is the process by which the proceeds of crime are sanitised 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.

3.2 Stages of money laundering

Money laundering schemes typically involve three distinct stages:

- ***placement*** – the process of getting criminal money into the financial system.

- ***layering*** – the process of moving the money within the financial system through layers of transactions; and

- ***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 Potentially suspicious transactions

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

- large cash payments.
- multiple small cash payments to meet a single payment obligation.
- payments or prospective payments from third parties, particularly where:
  - there is no logical connection between the third party and a student, or
  - the third party is not otherwise known to the University, or
  - a debt to the university is settled by various third parties making a string of small payments.
- payments from third parties who are foreign public officials or who are politically exposed persons ("PEP").
- payments made in an unusual or complex way.
- 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 can retain interest or otherwise retain a small sum.
- donations which are conditional on certain individuals or organisations, who are unfamiliar to the University, being engaged to carry out work.
- requests for refunds of advance payments, particularly where the University is asked to make the refund payment to someone other than the original payer.
- a series of small payments made from various credit cards with no apparent connection to a student and sometimes followed by chargeback demands.
- 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.
- prospective payers are obstructive, evasive, or secretive when asked about their identity or the source of their funds or wealth.
- prospective payments from a potentially risky source or a high-risk jurisdiction.

- 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 Principal Money Laundering Offences

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

- the principal money laundering offences under the Proceeds of Crime Act 2002.
- the prejudicing investigations offence under the Proceeds of Crime Act 2002; and
- 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.

5.2 Application of Money Laundering Offences & criminal property

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.
- 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 to:

- conceal, disguise, convert or transfer criminal property or to remove it from the United Kingdom.
- enter into an arrangement that you know, or suspect makes it easier for another person to acquire, retain, use or control criminal property; and
- acquire, use, or possess criminal property provided that adequate consideration (i.e. proper market price) is not given for its acquisition, use or possession.

  University employees 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.

5.3 Defences & responsibilities

In all three cases, University and the employees will only have a defence if the National Crime Agency does not refuse consent to the transaction or event.

The *employee* is responsible for making an authorised disclosure of the transaction to the Nominated Officer.

The Nominated Officer will provide instruction to the employee and is responsible for considering the requirement to contact the National Crime Agency.

5.4 Failure to Disclose Offence

It is a crime 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 they received the information.

5.5 The Offence of Prejudicing Investigations / Tipping-Off

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 up to five years imprisonment, to make a disclosure which is likely to prejudice the money laundering investigation. University employees can commit this offence if they tell a person an authorised disclosure has been made in their case.

This policy requires authorised disclosures to be kept strictly confidential. Any concerns and queries should be discussed with the Nominated Officer or in their absence their deputy only, and not discussed with any other individual, including Line Managers.

5.6 Know your Customer.

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.

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).

6. Terrorist Finance

6.1 The Principal Terrorist Finance Offences

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.

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.

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

- raising, possessing, or using funds for terrorist purposes.
- becoming involved in an arrangement to make funds available for the purposes of terrorism; and
- facilitating the laundering of terrorist money (by concealment, removal, transfer or in any other way).

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.

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.

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.

6.2 The Offence of Prejudicing Investigations

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. This policy requires disclosures under the Terrorism Act 2000 to be kept strictly confidential.

7. Procedures

7.1 Procedure overview

The University will:

- conduct an annual risk assessment to identify and assess areas of risk of money laundering and terrorist financing that are particular to the University.
- implement controls proportionate to the risks identified.
- establish and maintain policies and procedures to conduct due diligence on funds received.
- review policies and procedures annually and carry out on-going monitoring of compliance with them.
- appoint a Nominated Officer to be responsible for reporting any suspicious transactions to the National Crime Agency.
- provide training to all relevant employees, including temporary employees, on joining the University, and existing employees; and
- maintain and retain full records of work done in relation to this policy.

7.2 The University's Risk Assessment, Continuous Review and Accountability

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

- Conduct an assessment of money laundering and terrorist finance risk in the activities if the University.
- review and, if necessary, revise this policy in light of that risk assessment.
- 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
- report to Council on all aspects of this policy, including its implementation.

In order to facilitate the review and accountability functions, the Vice Chancellor will ensure:

- the availability of appropriate management information to permit effective oversight and challenge; and
- the maintenance and retention of full records of work done under this policy.

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

7.3 Transaction Due Diligence

Due diligence is the process by which the University assures itself of the provenance of funds it receives and how it can be confident that it knows the people and organisations with whom it works and receives funds from.

Due diligence should be carried out before the funds are received and funds must not be returned before due diligence has been reviewed.

In practical terms this means:

- identifying and verifying the identity of a payer or a payee, typically a student, sponsor, or a donor.
- 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.
- identifying and verifying the source of funds from which any payment to the University will be made.
- identifying and, in some circumstances, verifying the source of wealth from which the funds are derived.

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.

7.4 Transaction Risk Assessment

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

Where the case falls into the category of 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, by email, to the Nominated Officer.

The Nominated Officer will consider the report and will decide:

- whether or not to accept or to make the proposed payment.
- whether or not to make an authorised disclosure to the National Crime Agency; and
- whether or not to make a disclosure under the Terrorism Act 2000.

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.

7.5 Confidentiality of risk assessments

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 employees 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.

7.6 Monitoring

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 employees. Internal audit may be called upon to assist in monitoring effective implementation of this policy.

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.

7.7 Training

On joining the University all employees will receive anti-money laundering training as part of their induction process.

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.

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

8. Monitoring and Review

This policy will be reviewed and updated once every two years, or more frequently should an incident occur, or upon a change to UK legislation.

9. Associated policies

- Anti-Bribery and Corruption Policy
- Counter-Fraud Policy
- Criminal Finances Act Policy
- Fraud Response Plan
- HR Policies
- Whistle-Blowing Policy

Version control

Version	5.0
Amendments	Minor changes throughout the document for clarification purposes. This policy will be updated for name changes upon change of CFO without further requirement for approval.
Updated	29.01.26
Approval Date	
Approval Body	AUDIT, ASSURANCE & RISK COMMITTEE
Nominated Officer	Chief Financial Officer
Accountable Officer	Vice-Chancellor