# University of Warwick

# Anti-Money Laundering (AML) Policy

## Document Control:

| | |
|---|---|
| **Policy Owner:** | Chris Key, Deputy Finance Director |
| **Policy Author(s):** | Debbie Jay, Deputy Finance Director /Julia Porter, Head of Finance (Projects) |
| **Effective Date:** | 8 November 2023 |
| **Approving Body:** | Finance & General Purposes Committee – to approve<br>Policy Oversight Group – to note and monitor in accordance with Policy Framework |
| **Equality Impact Assessment Date:** | 27 August 2024 |
| **Version Number:** | V1.1 |
| **Date of Next Review:** | January 2026 |

## Amendment History:

| Version Number: | Effective Date: | Summary of Amendments: | Author: |
|---|---|---|---|
| v1.0 | 8 November 2023 | Inception of Policy | Debbie Jay, Deputy Finance Director |
| V1.1 | January 2025 | 1. Change of owner from Debbie Jay, Deputy Finance Director to Chris Key, Deputy Finance Director<br>2. Section 5.3: Update to reflect intended use of Form in Section 3 of Operating Procedures<br>3. Section 6.1 – updated to note cash payments are not accepted by the University. Link to high-risk country list inserted.<br>4. Update to Summary Flowchart. | Julia Porter, Head of Finance (Projects) |
| | | | |
| | | | |

## Contents



## 1. Introduction

1.1 This Policy is concerned with prevention of money laundering and terrorist or criminal financing in relation to the University of Warwick's activities both within and outside the UK. This Policy sets out the procedure to be followed if money laundering is suspected.

1.2 The University of Warwick (the "University") is committed to abiding by all relevant legislation including:

- the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017);
- the Money Laundering and Terrorist Financing (Amendment) Regulations 2019;
- the Criminal Finances Act 2017 (CFA 2017);
- the Terrorism Act 2000 (TA 2000) and
- the Proceeds of Crime Act 2002 (POCA 2002).

This legislation exists to prevent terrorists and other criminals from laundering money or otherwise dealing with criminal or terrorist property in a way that benefits them. Charities, including other HEIs, have been both targets and victims of terrorist or illegal activity. It is important therefore that the University remains vigilant and has a robust Policy in place to combat such activity. The legislative framework can be found at Appendix A of this Policy.

Money laundering is a criminal offence, with penalties of unlimited fines and/or terms of imprisonment ranging from two to fourteen years for those judged as being involved in money laundering including members of staff accepting such payments.

1.3 The UK Government produces a list of proscribed organisations concerned in terrorism, prohibited from operating in the UK, and a list of designated persons or entities who face financial restrictions in the UK. The list of proscribed terrorist organisations is held at https://www.gov.uk/government/publications/proscribed-terror-groups-or-organisations--2 .

A current list of those who are currently subject to financial sanctions for believed involvement in terrorist activity can be found at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/779688/Terrorism_and_Terrorist.pdf

1.4 Countries may also be subject to sanctions and embargoes by the EU, UN and Organisation of Security and Co-operation in Europe. All of the countries subject to total or partial restrictions of some kind are listed in Schedule 4 of the Export Control Order 2008. Further guidance on these countries can also be obtained from the HM Treasury website. Providing certain kinds of

support to a prohibited organisation or designated person will be an offence. The University must ensure that its premises, assets, staff, volunteers or other resources cannot be used for activities that may support or condone terrorism, or offences under the relevant legislation may be committed. The University also has a duty, in certain circumstances, to report any potential or actual suspicious activity. Failure to do so could result in a criminal offence being committed.

1.5 Any allegation that an employee of the University or one of its subsidiary companies has acted in a manner inconsistent with this Policy will be taken seriously and investigated. Employees of the University may be subject to disciplinary procedures for failure to comply with this Policy. The University reserves the right to terminate its contractual arrangements with any third-party providing services for or on behalf of the University where there is reasonable evidence that they/their staff have failed to follow this Policy.

## 2. What is money laundering?

2.1 Money laundering is the process of taking profits from crime and corruption and transforming them into legitimate assets. It takes criminally-derived 'dirty funds' and converts them into other assets so they can be reintroduced into legitimate commerce. By concealing the true origin or ownership of the funds, this will effectively 'clean' them.

2.2 Money laundering is defined as:

- concealing, disguising, converting, and/or transferring criminal property or removing it from the UK;
- entering into or becoming concerned in an arrangement which you know or suspect to facilitate the acquisition, retention, use or control of criminal property by or on behalf of another person; and/or
- acquiring, using or possessing criminal property.

2.3 In the UK**,** severe penalties are imposed on individuals connected with any stage of laundering money, including unlimited fines and/or terms of imprisonment ranging from 2 to 14 years. Offences include:

- failing to report knowledge and/or suspicion of money laundering;
- failing to have adequate procedures to guard against money laundering;
- knowingly assisting money launderers;
- tipping-off suspected money launderers; and
- recklessly making a false or misleading statement in the context of money laundering

2.4 In practice, an apparently legitimate and regular transaction - such as the payment of student fees and its subsequent refund - could disguise money laundering. It is therefore essential that the University has policies and procedures in place to ensure that the University does not become involved in money laundering by inadvertently legitimising suspect individuals or transactions.

## 3. Scope

3.1 This Policy applies to all individuals engaged in financial transactions for or on behalf of the University. It will therefore cover all staff of the University and all those third parties acting on its behalf, including but not restricted to agents, wherever they may be located. The Policy will also apply to students when they are acting on behalf of the University, either in a paid or voluntary role.

3.2 It is expected that individuals covered by this Policy will:

- ensure that they are familiar with this Policy;

- avoid handling any money, goods or other items known or suspected to be associated with the proceeds of crime;
- remain vigilant and report concerns immediately in line with this Policy;
- co-operate fully with any investigations; and
- maintain confidentiality about any suspected or actual incidents involving the University to avoid "tipping off".

3.3 If there are concerns about a breach of this Policy, the reporting procedure set out in section 5 should be followed.

3.4 The Operational Guidelines provide detailed information on risk assessment, customer due diligence and reporting of suspected money laundering transactions.

## 4. Risk Assessment

4.1 The University has adopted a risk-based approach towards anti-money laundering and undertaking appropriate due diligence. Although most of the University's financial activities could be considered as relatively low risk with regard to money laundering, all staff must be vigilant against the potential for such financial crime and fraud risks. Such risk assessment will take into consideration geographic and customer risk factors.

4.2 It is important that an assessment is undertaken of the risks of offences occurring under the relevant legislation. This enables areas of specific vulnerability to be identified and proportionate and prioritised mitigating actions to be put in place, recognising that risk will vary from sector to sector and depend on the location of the activity. Risk of non-compliance with terrorist financing legislation should be addressed through the University's risk management processes. It is important that this is done at all levels, and departments are required to assess the risks in relation to their activities. In addition, departments are asked to assess specific business transactions where there may be particular risks, for instance where third parties are acting on behalf of the University or where departments are dealing with individuals or organisations in areas where terrorist activity occurs. Departmental assessment of the risk of breaching terrorist financing laws must form an element of the due diligence undertaken when consideration is being given to entering into a business or academic partnership, acknowledging that such due diligence should be proportionate to the assessed risk. The University's risk management processes will also, therefore, assess the total risk portfolio as reported through departmental assessment mechanisms. Further guidance is available on the Finance Office website Anti-Money Laundering (warwick.ac.uk).

## 5. Reporting

5.1 The University is committed to ensuring there is a safe and confidential way of reporting any potential incidents.

5.2 Any concerns should be reported as soon as possible.

5.3 The University's specific reporting and procedures are as follows:

In the case of a known or suspected breach of this Policy or a concern surrounding a monetary transaction or a potential money laundering offence, individuals should:

- unless this would result in tipping off, report internally to your line manager or Head of Department.
- if, in consultation with your line manager (where appropriate), reasonable suspicion is confirmed a report should be made to the Finance Office using the form at Part 3 of the Operational Guidelines: Anti-Money Laundering (warwick.ac.uk). The report should contain as much detail as possible about all the people/companies involved, the nature of the transaction and why you are suspicious and any other relevant information.

- do not inform the party/entity concerned or anyone else (unless instructed by the Finance Director) that the suspicious transaction has been reported.

5.4 In the case of a breach of the Policy or potential offence under the relevant legislation occurring the University, through the Finance Office, will:

- Make reasonable enquiries, whilst avoiding tipping off those suspected of involvement.
- Suspend the transaction if one is still ongoing and it is deemed appropriate.
- Report any suspected breach of the Policy to the Group Finance Director and/or the Head of Internal Audit.
- Consider whether the University has a suspicion or knowledge of money laundering or terrorist financing which requires a Suspicious Activity Report to the National Crime Agency or some other form of disclosure.
- If necessary, contact HM Treasury Asset Freezing Unit to seek a licence or permission to deal with the funds.
- Consider whether a serious incident has occurred which should be reported to the Office for Students (OfS).

5.5 The University's Whistleblowing Code of Practice also permits staff and anyone contractually associated with the University to raise concerns of serious malpractice in the University, https://warwick.ac.uk/services/gov/whistleblowing

5.6 Any allegations of misconduct under this Policy within the jurisdiction of the University will be taken seriously. Should any member of the University be found to have acted in contravention of this Policy or the related UK legislation, action may be taken under the University's Disciplinary Procedures. Breach of this Policy may be considered an act of gross misconduct and where it is considered a criminal offence has occurred the police may be informed.

5.7 The Finance Director will keep a register of money laundering reports (and relevant documents), including any reports made to the National Crime Agency. Current guidance requires these reports and associated documentation to be kept for a minimum of six years.

## 6. High Risk Indicators

6.1 The presence of any of the factors below should trigger consideration under this Policy:

- Requests for refunds from students or their intermediaries or any legal entity.
- Payments from third parties, particularly where:
  - it is unclear as to the relationship with between the two parties,
  - the third party is not otherwise known to the University,
  - there are several small payments relating to a single transaction.
- Failure to take up places (after acceptance).
- Overpayments.
- Applications from high-risk countries, especially those named on the sanctions list.
- Agents who do not follow customary practice/normal procedures relating to deposits and tuition fees.
- Verification of an individual's identity is difficult.
- Behaviour by a student or legal entity that raises suspicions that money/property may have a criminal/terrorist source including failure to explain the source of funds or goods when reasonably asked.

- Any other facts which suggest that something unusual is happening and give reasonable suspicion about the motives of an individual.

A cash payment a from student or their intermediary or any legal entity or customer would also be considered a high-risk indicator, but cash payments are not accepted by the University.

6.2 A proposal to trade, commence research or student recruitment from a country against which potential sanctions/embargoes exist or which has a high-risk profile for other reasons should also trigger consideration under this Policy.

6.3 A list of sanctioned and high-risk countries is available on the Finance Office webpages Anti-Money Laundering (warwick.ac.uk)

6.4 A list of all financial sanctions imposed in the UK by country, administration or terrorist group is available at: https://www.gov.uk/government/collections/financial-sanctions-regime-specific-consolidated-lists-and-releases

It also includes guidance as to what is prohibited under each financial sanction.

## 7. Know Your Customer (KYC) and Customer Due Diligence (CDD), including Financial Sanctions Targets

7.1 The University must be reasonably satisfied as to the identity of customers and other parties involved in business relationships with the University. This encompasses knowing the name, permanent address and/or date of birth, as part of the Customer Due Diligence process, before commencing a business relationship. For example, this could include obtaining a copy of photo-identification and proof of address. This should also include identifying any beneficial owner(s) (where appropriate). Ongoing monitoring of the business relationships should be conducted as part of continuing due diligence. The level of Customer Due Diligence will vary in line with the perceived risk associated with the proposed transactions/business relationship.

7.2 Undertaking Know Your Client and Customer Due Diligence will ensure the University complies with the law, as well as helping to ensure that the University does not enter into student and other relationships that might be considered too risky.

7.3 Enhanced Customer Due Diligence will be required for relationships with Politically Exposed Persons (PEP's).

7.4 Further information on CDD is available in the Operational Guidelines at Anti-Money Laundering (warwick.ac.uk).

## 8. Records

8.1 The Regulations require the University to take reasonable care to make and keep adequate records (including customer identification and accounting records) which are appropriate to the scale, nature and complexity of the University's business. These records typically include identity documents, transaction records, records of reports (internal and external), and training records. The relevant retention periods are specified in the University's Financial Procedure 5.

## 9. Monitoring and Review

9.1 The University is committed to reviewing on an ongoing basis the effectiveness of its policies and procedures in relation to Anti Money Laundering and criminal financing measures. The Policy will be subject to annual review.

## Summary – Reporting Process

A high risk indicator is present, as set out in section 6, or other behaviour/circumstances raises suspicions that money/property may have a criminal/terrorist source.

**All staff:**

- Unless this would result in tipping off, report your discovery to relevant line manager or Head of Department.
- Seek assistance from the Finance Office by emailing AML@warwick.ac.uk if required .
- If money laundering is suspected, complete form in Part 3 of the Operational Guidelines with as much information as possible and send to the Finance Office using the Contact Details provided on the form.
- Do not inform the party/entity concerned or anyone else (unless instructed by the Finance Director) that the suspicious transaction has been reported

**The Finance Office will:**

- Make reasonable enquiries, whilst avoiding tipping off those suspected of involvement.
- Depending on the results of the enquiries, allow or suspend the transaction.
- Report any suspected breach of the Policy to the Group Finance Director and/or Head of Internal Audit.
- Consider whether the University has a suspicion or knowledge of money laundering or terrorist financing which requires a Suspicious Activity Report to the National Crime Agency or some other form of disclosure. The United Kingdom Financial Intelligence Unit (UKFIU) produce a Guidance Note "Introduction to suspicious Activity reports" which may be helpful.
- If necessary, contact HM Treasury Asset Freezing Unit to seek a licence or permission to deal with the funds.
- Consider whether a serious incident has occurred which should be reported to the Office for Students.

## Application of this Policy to sanctions/embargoes list countries

A proposal exists to commence:

(i) research;

(ii) student recruitment;

(iii) commercial transactions with legal entities/individuals;

within a country against which sanctions/embargoes exist or which has a high risk profile for other reasons.

Separate government guidance will exist for each individual country on the sanctions/embargoes list.

Particular care should be taken during ***medical*** and ***scientific projects*** or ***those involving the use of computer hardware/software and technology*** as these areas often attract prohibitions.

Check guidance for the relevant country:

- Are any of the proposed actions proscribed by the guidance?
- Are any of the goods the university will use during the proposed action proscribed by the guidance?
- Are any of the proposed actions taking places within industries for which support is proscribed? e.g. the oil, gas or petroleum producing industries?
- Contact the Finance Office at fincompliance@warwick.ac.uk for assistance

YES

The proposed action is not permitted under sanctions law and should not be permitted.

NO

The proposed action is likely to be permitted to go ahead but any further concerns or suspicions should be checked with your line manager/ the Finance Office.

# Appendix A - The Legislative Framework

Various duties and offences arising under the relevant legislation include:

## 1. Terrorism Act 2000:

The TA 2000 sets out a number of offences and duties, the most relevant of which are contained in sections 15 to 19.

These sections create offences of fundraising, using money/property or entering into an arrangement to make money/property available to another, with intent or reasonable suspicion that it may be used for the purposes of terrorism.

An offence takes place if a person enters into or becomes concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property: (i) by concealment (ii) by removal from the jurisdiction (iii) by transfer to nominees (iv) in any other way.

The act also creates a legal duty to disclose to the police any belief or suspicion, based on information obtained in the course of a trade, profession, business or course of employment, that another person has committed any of the offences mentioned above. This disclosure must be made as soon as is reasonably practicable to any police constable, a member of the National Crime Agency, or by phoning the anti terrorist hotline. Also, any person may disclose to the police a suspicion or belief that any money/property is, or derived from, terrorist property and any matter on which this suspicion or belief is based.

## 2. Proceeds of Crime Act 2002:

POCA 2002 creates a number of money laundering offences all relating to dealing with criminal property, that is, property of any kind, including money, obtained as a result of a criminal lifestyle. Much of the act applies only to financial institutions but everyone, including the University, must adhere to the sections mentioned below.

Sections 327-329 create offences of dealing with criminal property by: (i) concealing, disguising, converting, transferring or removing criminal property from the jurisdiction; (ii) becoming concerned in an arrangement which he knows or suspects facilitates the acquisition, retention, use or control of criminal property by another; and (iii) acquiring, using or having possession of criminal property.

There is an inter-relationship between the POCA offences and terrorist offences in that any funds acquired through or in advance of terrorist purposes may also be criminal property and subject to the money laundering laws. Therefore, any suspicion that a person or other entity the University has dealings with is involved in terrorism may also engage POCA laws in relation to dealing with any funds or other property of that person/entity, creating multiple offences. The POCA laws are also important in that they create a duty to disclose if the University knows or suspects that someone is engaged in money laundering. Disclosure is made by making a Suspicious Activity Report (SAR) to the National Crime Agency through their SAR online system before any further steps are taken to deal with the property. The University must not tell the person or entity suspected that a SAR has been made.

## 3. Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (and the Money Laundering and Terrorist Financing (Amendment) Regulations 2019)

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.

The University has a responsibility to:

- make relevant individuals aware of this Policy;
- implement a procedure to enable the reporting of suspicious activity;
- maintain customer due diligence and identification procedures to 'know your customer', in relevant circumstances; and
- maintain adequate records of transactions.

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

- passport and/or visa;
- birth certificate; or
- other official document.

If an organisation is not known to the University, you should:

- look for letter headed documents;
- check that invoices show a company's registered office and VAT number;
- check against the LexisNexis Risk Management Solutions database;
- check websites, for example, www.companies-house.gov.uk; or
- aim to meet or contact key sponsors if you feel appropriate to verify validity of contact.

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

If there are any doubts about identity, these suspicions should be reported (see section 5) and you should not continue to act.

## 4. Criminal Finances Act 2017

The CFA 2017 has made all businesses and organisations, including universities, criminally liable if they fail to prevent tax evasion by either a member of their staff or an external agent, even where the business/ organisation was not involved in the act or was unaware of it. Amongst other measures, the CFA 2017 introduces a new corporate criminal offence of failing to prevent the facilitation of tax evasion.

All corporates are affected and can be subject to prosecution for the facilitation of tax evasion by "associated persons". "Associated persons" include the University's officers, employees, workers, agents, sub-contractors or other people or organisations that provide services for or on the University's behalf.

Under the CFA 2017, in the event of there being both:

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

The University will automatically be charged with the offence of failing to prevent its representatives from committing the criminal act of facilitation unless it can demonstrate that it had reasonable procedures in place to prevent that facilitation.

The University, if found guilty, could face an unlimited fine, exclusion from tendering for public contracts, and damage to its reputation.

The University has a zero tolerance approach to the facilitation of tax evasion and will not work with any individual or organisation that is not committed to preventing the facilitation of tax evasion, in compliance with the Criminal Finances Act 2017.

All cases of suspected facilitation of tax evasion by an associated person will be thoroughly and promptly investigated.