Version number: 1.0

Policy owner: Director of Finance

Effective date: 24/10/2023

Review date: 23//10/2028

Previous version: First version

University of Chichester

# Anti-Money Laundering and Counter Terrorist Financing Policy

**Approved by the Vice Chancellor’s Group on XX XXX 2023**

**Contents**

1 POLICY AIMS 3

2 IMPLEMENTATION 3

3 WHAT IS MONEY LAUNDERING? 3

4 MONEY LAUNDERING WARNING SIGNS OR RED FLAGS 4

5 MONEY LAUNDERING - THE LAW 4

6 THE PRINCIPAL MONEY LAUNDERING OFFENCES 5

7 DEFENCES 5

8 FAILURE TO DISCLOSE OFFENCE 5

9 THE OFFENCE OF PREJUDICING INVESTIGATIONS / TIPPING-OFF 5

10 THE MONEY LAUNDERING, TERRORIST FINANCING & TRANSFER OF FUNDS 5

11 THE PRINCIPAL TERRORIST FINANCE OFFENCES 6

12 PROCEDURE OVERVIEW 6

13 TRANSACTION DUE DILIGENCE 7

14 TRANSACTION RISK ASSESSMENT 7

15 MONITORING 8

16 TRAINING 8

17 TRANSACTION DUE DILIGENCE AND RISK ASSESSMENT PROCEDURE 8

**Introduction**

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. This process conceals the true origin or ownership of the funds, and so 'cleans' them.

1. ***Policy Aims***

This policy supports the University in its aim to comply fully with all UK legislation and all relevant overseas legislation in relation to Anti Money Laundering and to ensure it minimises the risk of money-laundering taking place in its operations.

For the avoidance of doubt, the University will not do business with anyone whom it is suspects of taking part in any activity, knowingly or unknowingly, which it regards as linked with potential money-laundering.

1. ***Implementation***

The Director of Finance is directly responsible to the Vice-Chancellor’s Group for the implementation of this policy and will ensure the following:

1. appropriate due diligence is conducted by the student application process collating data around payers and source of funds
2. anti-money laundering and counter-terrorist finance training is undertaken by relevant University staff via British Universities Finance Directors Group (BUFDG); and
3. this policy is reviewed every 5 years and up-dated sooner if necessary and levels of compliance are monitored.

Certain functions under this policy are to be undertaken by a Nominated Officer. For the purposes of this policy, the Nominated Officer is the Financial Services Manager and, in their absence, Head of Financial Control.

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.

1. ***What is Money Laundering?***

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:

1. placement – the process of getting criminal money into the financial system;
2. layering – the process of moving the money within the financial system through layers of transactions;
3. 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***

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:

1. large cash payments;
2. multiple small cash payments to meet a single payment obligation;
3. payments or prospective payments from third parties, particularly where
   1. there is no logical connection between the third party and the student, or
   2. where the third party is not otherwise known to the University, or
   3. where a debt to the university is settled by various third parties making a string of small payments;
4. payments made in an unusual or complex way;
5. 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;
6. donations which are conditional on particular individuals or organisations, who are unfamiliar to the University, being engaged to carry out work;
7. requests for refunds of advance payments, particularly where the University is asked to make the refund payment to someone other than the original payer;
8. a series of small payments made from various credit cards with no apparent connection to the student and sometimes followed by chargeback demands;
9. 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;
10. prospective payers are obstructive, evasive or secretive when asked about their identity or the source of their funds or wealth;
11. prospective payments from a potentially risky source or a high-risk jurisdiction;
12. the payer’s ability to finance the payments required is not immediately apparent or the funding arrangements are otherwise unusual.
13. ***Money Laundering - The Law***

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

1. the principal money laundering offences under the Proceeds of Crime Act 2002;
2. the prejudicing investigations offence under the Proceeds of Crime Act 2002; and
3. 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 University is required to comply with the Proceeds of Crime Act 2002. The University is not authorised or regulated by the Financial Conduct Authority. It therefore does not have to comply with Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, but it is considered best practice for it to do so.

1. ***The Principal Money Laundering Offences***

These offences, contained in the 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, severe penalties can be imposed on both the University and its employees, to:

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

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.

1. ***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.

1. ***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 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. University staff can commit this offence if they tell a person an authorised disclosure has been made in their case.

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

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 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.

**Terrorist Finance**

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.

The Terrorism Act 2000 create offences of:

1. raising, possessing or using funds for terrorist purposes;
2. becoming involved in an arrangement to make funds available for the purposes of terrorism; and
3. 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.

The Terrorism Act 2000 creates an offence, 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 the Terrorism Act 2000 and does not then report the matter either directly to the police or otherwise in accordance with their employer’s procedures.

**OUR PROCEDURES**

1. ***Procedure Overview***

The University will:

1. As part of the University Risk Management Register, conduct an annual risk assessment to identify and assess areas of risk money laundering and terrorist financing particular to the University;
2. implement controls proportionate to the risks identified;
3. establish and maintain policies and procedures to conduct due diligence on funds received;
4. review policies and procedures periodically and carry out on-going monitoring of compliance with them;
5. appoint a Nominated Officer to be responsible for reporting any suspicious transactions to the National Crime Agency;
6. provide training to all relevant members of staff, on joining the University, and provide annual refresher training.
7. ***Transaction Due Diligence***

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.

For International payments; all payments should be made through the University’s Payment Portal – checks are performed by the Portal provider to ascertain if funds are being transmitted from high risk jurisdictions or from sanctioned individuals – this forms part of the University due diligence.

In practical terms this means:

1. identifying and verifying the identity of a payer or a payee, typically a student or a donor;
2. 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;
3. identifying and verifying the source of funds from which any payment to the University will be made; and
4. identifying and in some circumstances verifying the source of wealth from which the funds are derived.

The above is achieved by questionnaires completed by the student via the following:

International student for deposits – Applicants Payment Portal

All students when completing registration – ChiView

1. ***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.

If the transaction raises suspicion of money laundering or terrorist finance, this must be reported to the Nominated Officer as soon as practicable.

The Nominated Officer will consider the transaction and will decide:

1. whether or not to accept or to make the proposed payment;
2. whether or not to make an authorised disclosure to the National Crime Agency; and
3. 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.

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

1. ***Monitoring***

The Director of Finance 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 reports and feedback from staff.

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.

1. ***Training***

On joining the University any staff whose duties will include undertaking an AML function will receive anti-money laundering training as part of their induction process and annual refresher anti-money laundering and counter-terrorist finance training via BUFDG.

The AML training will be mandatory for staff in specific roles within the Finance Department e.g. Sales Ledger, Financial Services Manager and Head of Financial Control.

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

1. ***Transaction Due Diligence and Risk Assessment Procedure***

**Step 1 – Due Diligence - Identify the Person, Source of Funds and Source of Wealth**

The University has a robust "know your customer" process for students and other customers, including international students.

Student ID is checked during admission for international students and registration for UK students, including checks that valid visas are in place where required. Credit checks should be performed on commercial sponsors via our external credit rating agency prior to being approved as a customer or sponsor. Schools and other government institutions (UK & Non-UK) are considered low risk sponsors and do not require credit checking.

1. No cash is accepted for tuition or accommodation fees
2. Suspicious payment reports from the University’s card payment gateway provider are monitored daily and investigated where necessary
3. No refunds can be made other than to the original payer without further identity checks being conducted AND with the student’s express permission
4. Unallocated payments purporting to be from students are returned to source where no registered student ID is provided
5. Other than in exceptional circumstances, refunds are only made using the original mode of payment
6. Any potential breaches of this policy must be flagged to the University's Nominated Officer

**Step 2 – Risk Assessment**

Acting in accordance with this policy, the University has assessed risk at two different levels.

*Tier 2 Risk*

* Home student whose tuition fees are paid directly to the University by the Student Loan Company.
* Students whose personal circumstances give rise to no cause for concern, whose payments to the University are made from a regulated account held in their own name and where they live, and where the source of funds gives rise to no basis for suspicion.
* Students whose payments are made by a third party, where there is a good reason for the third party wanting to make the payment and where the third party and their source of funds and source of wealth present no money laundering risk

*Tier 1 Risk*

* All cases not falling within Tier 2.

**Step 3 – Further Due Diligence for Tier 1 risks**

Where the case presents a Tier 1 risk further enquiries will be required to ensure that the University has as much information as possible when making a final assessment of the money laundering or terrorist finance risk the student poses.

**Responsibilities of the Nominated Officer**

Following the due diligence exercise, if it is suspected that a payment or proposed payment involves money laundering or terrorist finance, an authorised disclosure of the matter must be made to the National Crime Agency via the NCA Suspicious Activity Report online portal.

At no time and under no circumstances should any suspicions be voiced to the person(s) suspected of money laundering.

Where the Nominated Officer concludes that there are no reasonable grounds to suspect money laundering then consent will be given for transactions to proceed and the decision will be recorded as such.

Details of the reporting to the NCA can be found at:

<https://www.gov.uk/guidance/money-laundering-regulations-report-suspicious-activities>

NCA Suspicious Activity Report online portal:

<https://www.ukciu.gov.uk/>