ANTI MONEY LAUNDERING AND COUNTER TERRORIST FINANCING POLICY

1. Introduction

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.

1.2 The Pro Vice Chancellor (Finance & Resources) is directly responsible to the Vice Chancellor and Chief Executive for the implementation of this policy. As such, with the Vice Chancellor and Chief Executive's full support, (s)/he will ensure regular assessments of the University's money laundering and terrorist finance risks are conducted, and relied upon to ensure the effectiveness of this policy and that appropriate due diligence is conducted. As a result of this, risks relating to individual transactions are assessed, mitigated and kept under review.

1.3 Certain functions under this policy are to be undertaken by a Nominated Officer. For the purposes of this policy, the Nominated Officer is the Principal Accountant – Finance Operations.

1.4 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 policies, as appropriate. Note that any such failures also expose the individual concerned to the risk of committing a money laundering offence.

2. What is Money Laundering?

2.1 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.

3. Money Laundering Warning Signs or Red Flags

3.1 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:

- 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 the student, or where the third party is not otherwise known to the University, or where 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 is allowed to retain interest or otherwise retain a small sum;
- donations which are conditional on particular 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 the 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.
- a potential supplier submits a very low quotation or tender. In such cases, the business may be subsidised by the proceeds of crime with the aim of seeking payment from the University in "clean money".

4. Money Laundering - The Law

4.1 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

4.2 These offences, contained in sections 327, 328 and 329 of 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, with a potential for a maximum punishment of a custodial sentence, 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.

4.3 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

4.4 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

4.5 It is a crime, with a potential for a maximum punishment of a custodial sentence, 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.

4.6 Section 6 of this policy sets out how such disclosures are to be made.

The Offence of Prejudicing Investigations / Tipping-Off

4.7 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 of the Proceeds of Crime Act 2002 provides that it is a crime, with a potential for a maximum punishment of a custodial sentence, 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. Section 6 of 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

4.8 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, with a potential for a maximum punishment of a custodial sentence, 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. Terrorist Finance

The Principal Terrorist Finance Offences

5.1 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.

5.2 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.

5.3 Sections 15 to 18 Terrorism Act 2000 create offences, with a potential for a maximum punishment of a custodial sentence, 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).

5.4 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.

5.5 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.

5.6 Section 19 Terrorism Act 2000 creates an offence, with a potential for a maximum punishment of a custodial sentence, 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 section 6.

The Offence of Prejudicing Investigations

5.7 Section 39 Terrorism Act 2000 creates an offence, with a potential for a maximum punishment of a custodial sentence, 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. Section 6 of this policy requires disclosures under the Terrorism Act 2000 to be kept strictly confidential.

6. OUR PROCEDURES

6.1 The University has carried out a risk assessment to identify and assess areas of risk money laundering and terrorist financing particular to the University and in doing so has set the following controls:

i) Cash will not be accepted for payment of tuition and accommodation fees;
ii) For other transactions, cash to the maximum value of £500 will be taken at FirstPoint, and loans to the maximum value of £500 will be paid out in cash;
iii) Where payments from potential international students are received, any subsequent return of funds due to non-enrolment will be returned either by refund of the credit card transaction via the Merchant website, or the payee's original bank account via a direct instruction by the University's bank to return the funds, as opposed to the University processing a refund transaction. This helps to ensure that no individual is able to treat the return of funds as a 'clean' payment from the University.

6.2 In conducting the assessment of money laundering and terrorist financing risk arising from the University's work and funding activity, the Pro Vice Chancellor (Finance & Resources) will have regard to the University's experiences and to any lessons learned in applying this policy. (S)/he 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. (S)he may also have regard to reports by non-governmental organisations and commercial due diligence providers.

Transaction Risk Assessment

6.6 Where the member of staff dealing with the case gives cause for further investigation, they must report this to the Nominated Officer.

6.7 The Nominated Officer will undertake further investigation and will provide a circumstances report to the Pro Vice Chancellor (Finance & Resources) who will then assess if there is cause for suspicion under the regulations. If the case falls into the category of suspicious the Nominated Officer will then report the case as soon as practicable to the National Crime Agency.

6.8 The Pro Vice Chancellor (Finance & Resources) in conjunction with the Nominated Officer will consider the circumstances 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.

6.9 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.

6.10 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.

6.11 In conjunction with the consideration of Money Laundering activities, the University will also consider the possibility of a transaction being fraudulent. Please see the University's Fraud Policy for further details Policies and Procedures.

Monitoring

6.12 The Pro Vice Chancellor (Finance & Resources) 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.

6.13 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.

Owner	Rob Bonham – Pro Vice Chancellor (Finance & Resources)
Approved By	UEB and Audit Committee
Approval Date	UEB - 12/03/2024 Audit Committee 19/03/2024
Version	1.0
Created	February 2024
Next Review Date	February 2026