TEESSIDE UNIVERSITY

ANTI-MONEY LAUNDERING (AML) POLICY

Document Title: Anti-Money Laundering (AML) Policy			
Version No.	v5.0	Policy Owner	Director of Finance & Commercial Development
Superseded version	Updates Anti-Money Laundering Policy v4.0 (April 2020)	Author Role Title	Deputy Director of Finance & Commercial Development (Financial Services & Assurance)
Approval Date	27 April 2021	Approved by	Audit Committee
Effective Date	27 April 2021	Review Date	April 2022

1. Introduction

1.1 The University and its subsidiary companies (the University) are committed to the highest standards of ethical conduct and integrity in their business activities in the UK and overseas. 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 outlines how the University and its employees will manage money laundering risks and comply with its legal obligations

1.2 The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017) transposes the Fourth EU Money Laundering Directive into UK Law. These obligations impact on certain areas of the University's business and, as under the previous regulations of 2007, require organisations to maintain internal procedures to prevent the use of their services for money laundering.

1.3 The University has a zero tolerance approach to money laundering and serious action will be taken against anyone found to be involved in money laundering, up to and including dismissal under the University's disciplinary processes.

2. Purpose and Scope of this Policy

2.1 This policy applies to ALL University staff and Governors, and covers University activities undertaken in the UK or overseas. Potentially any member of staff could be committing an offence under the money laundering laws if they suspect money laundering or if they become involved in some way and do nothing about it.

2.2 This policy sets out the procedures to be followed if money laundering is suspected, and defines the responsibility of both the University and individual employees in the process. It enables the University to comply with its legal obligations.

2.3 This policy outlines the University's arrangements to comply with the five key requirements of the money laundering regulations which are :

- All organisations must obtain satisfactory evidence of the identity of each customer with whom it deals with and/or has a business relationship
- This evidence of client identity must be retained for the duration of the client relationship and for a period of five years after it terminates; details of transactions must be kept for the same period
- Any suspicious transaction, whether in connection with a new or existing client, must be reported immediately to the Money Laundering Reporting Officer (MLRO)
- The MLRO must, if deemed appropriate, report suspicion of money laundering to the appropriate authorities; in the UK this is the National Crime Agency (NCA)
- Appropriate training must be provided to all relevant members of staff who handle, or are responsible for handling, any transactions with the

organisation's clients and counterparties to ensure that they are aware of the organisation's procedures which guard against money laundering and the legal requirements of the money laundering rules

2.4 The University's procedures are designed to ensure compliance with all of these requirements on a risk-sensitive basis for prevention of financial crime and money laundering, as detailed in this policy.

2.5 It is a requirement for all staff members, on an annual basis, to read this policy and provide a confirmation thereof to the MLRO through MyCompliance .

2.6 This Policy does not form part of any contract of employment and the University may amend it at any time.

3. What is Money Laundering?

3.1 Money laundering is the process of taking profits from crime and corruption and transforming them into legitimate assets. Money laundering takes criminally-derived 'dirty funds' and 'sanitises' 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. It also covers money, come by legitimate means, which is used to fund terrorism (reverse money laundering). 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. There are three stages in money laundering:

- Placement - proceeds of criminal activity are introduced into the financial system by some means;
- Layering - a financial transaction to distance the money from the illegal source;
- Integration - re-introduction of the illegal proceeds into legitimate commerce by providing an apparently-genuine explanation for the funds.

3.2 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 for:

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

3.3 Most anti-money laundering laws that regulate financial systems link money laundering (which is concerned with source of funds) with terrorism financing (which is concerned with destination of funds).

3.4 Whilst the risk to the University of contravening the legislation is low, it is extremely important that all employees are familiar with their legal

responsibilities. The key requirement on employees is to promptly report any suspected money laundering activity to the MLRO.

3.5 The University is fully committed to ensuring that there is a safe and confidential method of reporting any suspected wrongdoing to nominated officers. The University's Public Interest Disclosure Policy (''Whistle-blowing'') which is available on:

https://unity3.tees.ac.uk/Departments/USEC/UniversityRegulations/University%20Regulations%20Documents/Forms/New%20or%20Revised%20Regulation%20since%20September%202012.aspx

also permits employees and anyone contractually associated with the University to raise concerns of malpractice in the University, and those involving partners or competitors.

3.6 The University offers mentoring, advice or counselling to those who have reported a concern, where appropriate. Further information is available from the HR department.

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.

5.2 The Principal Money Laundering Offences

5.2.1. 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.

5.2.2 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.

5.3 Defences

5.3.1. In all three cases, there is a defence if there has been an authorised disclosure of the transaction either to the MLRO or to the National Crime Agency and the National Crime Agency does not refuse consent to it.

5.4 Failure to Disclose Offence

5.4.1. It is a crime, punishable by up to five years imprisonment, for a MLRO 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.

5.4.2 At section 14 below, this policy sets out how such disclosures are to be made.

5.5 The Offence of Prejudicing Investigations / Tipping-Off

5.5.1 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 section 13.5 below, this policy requires authorised disclosures to be kept strictly confidential.

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

5.6.1 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.

5.7 Terrorist Finance - The Principal Terrorist Finance Offences

5.7.1. 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. Therefore, the source of the funds concerned is immaterial, and it is the purpose for which the funds are intended that is crucial.

5.7.2 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.

5.7.3 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).

5.7.4 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.

5.7.5 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.

5.7.6 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 section 14 below.

5.8 **The Offence of Prejudicing Investigations**

5.8.1 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 section 13.5 below, this policy requires disclosures to be kept strictly confidential**.**

6. Personnel Responsible for the Policy

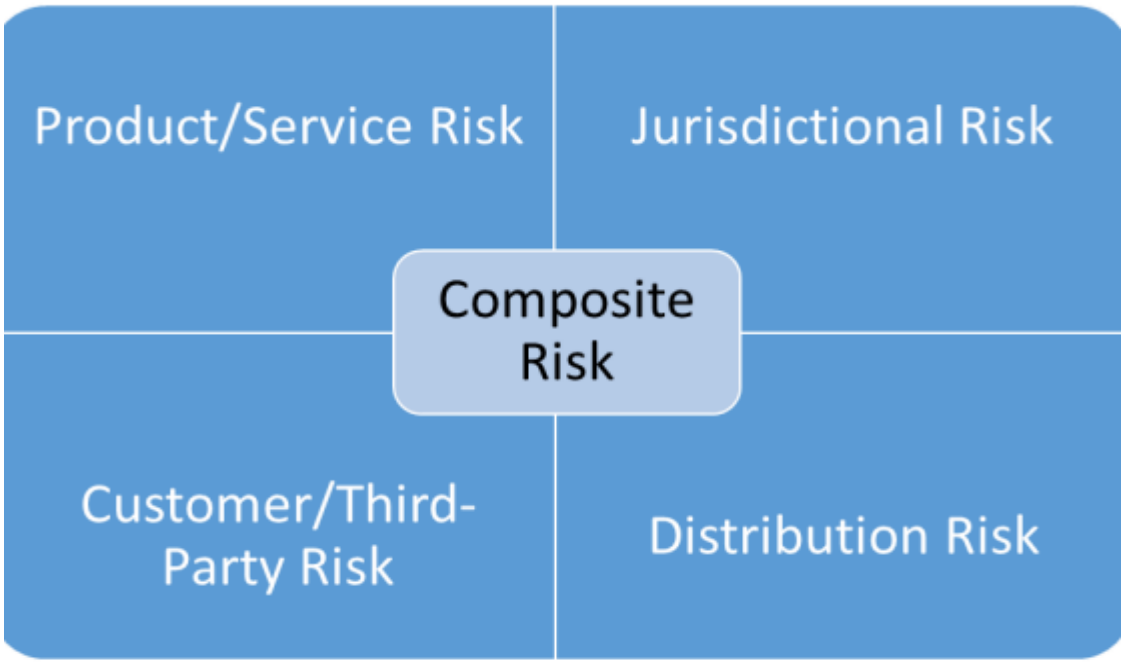
6.1 The University's Audit Committee has overall responsibility for this Policy and for reviewing the effectiveness of actions taken in response to concerns raised under this Policy. This Policy has been endorsed by the University's Executive Team.

6.2 The Director of Finance & Commercial Development has day-to-day operational responsibility for this Policy.

7. Anti- Money Laundering Risk Assessment

7.1 MLR 2017 requires the University to undertake a risk assessment, and to demonstrate and document that it was carried-out and has been/will be kept up-to-date.

7.2 A risk assessment has been undertaken of the University's current activities, as outlined in Appendix A. The University's AML controls and processes have to be in proportion to the financial crime risks and relate to the four primary sources of risks, shown in the diagram below. Taken together, these identify the overall or composite risk:



7.3 The four risks are:

- **Product/Service** Risks associated with our standard product and service offerings.
- **Jurisdictional** Risks associated with geography, location and jurisdiction including, but not limited to, the University's countries of operation, the location of customers, suppliers and/or agents, and transactional sources/destinations.
- **Customer/Third-Party** Risks associated with the people and/or organisations that we undertake business (in all forms) with including customers/third-parties, beneficial owners, agents, contractors, vendors and suppliers. Politically Exposed Persons (PEP's) and Sanctioned Parties are also considered within this risk.
- **Distribution** Risks associated with how we undertake business, including direct and indirect relationships (e.g. via an agent or third-party), face-to-face, digital/online and telephonic

7.4 The University adopts a risk-based approach towards anti-money laundering and conducting due diligence. Risk mitigation processes adopted by the University are:

- This policy is proportionate to the specific risks identified
- This policy has been approved by the Audit Committee
- There are both internal controls (with the University Secretary responsible for MLR 2017) and external controls such as the banks who monitor and prevent transactions with sanctioned regimes
- The University has agreed customer due diligence ('CDD') procedures for transacting with students, customers and third parties
- Reporting procedures, record keeping and monitoring of risk areas are in place
- This policy is reviewed and updated annually and reported to Audit Committee

8. Customer due diligence (CDD)

8.1 Customer 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. The Regulations require that the University must be reasonably satisfied as to the identity of the customer (and others) that they are engaging in a business relationship. Therefore, the University has policies and procedures for performing CDD, and the transaction monitoring arrangements on a risk-managed basis with systems and controls in place to mitigate any financial crime risks. As required by the MLR 2017, we can demonstrate and have documented the risk assessment in Appendix 1 which will be reviewed annually.

8.2 Our customer due diligence follows the principles of Know Your Customer (KYC), one of the fundamental precepts of global anti-money laundering regulations. This due diligence process identifies business relationships and customers and, hence, ascertains relevant information whereby the identity of a new customer (the 'beneficial owner') must be established before a business or financial relationship can begin or proceed. The three components of KYC are explained in Appendix 2. We retain the CDD records relied on for at least five years from the date on which reliance commences as failure to do so is a criminal offence.

8.3 Both customer and geographical risk factors need to be considered in deciding the level of due diligence to be undertaken. Simplified customer due diligence is appropriate where the University determines that the business relationship or transaction presents a low risk of money laundering or terrorist financing, taking into account our risk assessment. Under the UK's Money Laundering Regulations enhanced due diligence (EDD) is mandated for any business relationship with a person established in a high-risk third country.

Until the end of the Brexit transition period, the list of high-risk countries was determined by the EU under the 4th Anti Money Laundering Directive.

From 1 January 2021, the UK has had its own standalone list. Since then, any amendments made by the European Union to their list do not have effect in the UK. The current list of high-risk countries includes the 22 grandfathered from the assessments under the EU's 5th Money Laundering Directive and are:

- Afghanistan
- The Bahamas
- Barbados
- Botswana
- Cambodia
- Democratic People's Republic of Korea (DPRK
- Ghana
- Iran
- Iraq
- Jamaica
- Mauritius

- Mongolia
- Myanmar
- Nicaragua
- Pakistan
- Panama
- Syria
- Trinidad and Tobago
- Uganda
- Vanuatu
- Yemen
- Zimbabwe

8.4 The UK government publishes frequently-updated guidance on financial sanctions targets, which includes a list of all targets. This list can be found at:

https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets

The list provides information to assist in deciding whether the University is dealing with someone who is subject to sanctions. The University will ensure that it has no relationship with any individuals on this list.

9. Application of MLR 2017

9.1 MLR 2017 applies to cash transactions in excess of 10,000 Euros. For the purpose of this policy, this is set at a sterling equivalent of £7,500. However, the Proceeds of Crime Act applies to all transactions and can include dealings with agents, third parties, property or equipment, cheques, card, cash or bank transfers.

9.2 Particular rules apply to foreign students, and the immigration service needs to be notified if a student with a visa discontinues their study. These cases should be dealt with by the International Compliance Team in the normal course of business.

9.3 Cash payments

It is best practice to avoid accepting large cash payments for reasons associated with security and the risks associated with money laundering. It is therefore the University's policy not to accept cash payments above £2,500 for any purposes including the payment of accommodation or tuition fees.

9.4 Requests for refunds

9.4.1 Precautions should also be taken in respect of refunds requested following a payment by credit card or bank transfer. In these cases, refunds must only be made by the same method to the same account. In the event of an attempted payment by credit or debit card being rejected, the reason should be checked prior to accepting an alternative card. If in any doubt about the identity of the person attempting to make a payment the transaction should not be accepted.

9.4.2 Fees paid in advance by overseas students who have subsequently been refused a visa are only refundable providing appropriate documentary evidence is available to demonstrate the circumstances. Refunds should only be made to the person making the original payment, other than in exceptional circumstances where this is not possible.

9.4.3 Students must make arrangements to cover their own living expenses. If a sponsor or third party pays funds in excess of tuition fees for such purposes, the funds cannot be transferred to the student. The funds can only be repaid by the same method and to the same account as the original payment was made, other than in exceptional circumstances where this is not possible.

10. What the University will do:

Under the Money Laundering Regulations 2017 the University has a responsibility to:

Requirement	Response
10.1 Appoint a Money Laundering Reporting Officer (MLRO) to receive, consider and report as appropriate, disclosure of suspicious activity reported by employees.	The University has appointed the University Secretary as the nominated MLRO. In the absence of the University Secretary, the Director of Finance & Commercial Development will act as MLRO.
10.2 Implement a procedure to enable the reporting of suspicious activity, such as complex or unusually large transactions, or unusual patterns of transactions which have no apparent economic or visible lawful purpose.	The MLRO will implement and maintain an Anti-money laundering procedure. They will: • receive reports of suspicious activity from any employee in the business; • respond to reports of suspected money laundering activity; • consider all reports and evaluate whether there is - or seems to be - any evidence of money laundering or terrorist financing; • report any suspicious activity or transaction to the National Crime Agency ('NCA') using its SAR ('Suspicious Activity Report') Online system; • ask NCA for consent to continue with any transactions that they have reported and make sure that no transactions are continued illegally.
10.3 Maintain customer identification procedures in relevant circumstances.	It is important that controls are in place to identify the student, customer or other party dealing with the University. This is done during enrolment checks so checking identity to a valid University ID card is considered

	adequate evidence of identity for making payments to the University. • Where a payment is made on behalf of a student, then evidence of the payer's identity and relationship to the student concerned must be obtained. • If a person or an organisation is not known to the University look for letter headed documents, check web sites, request credit checks, or aim to meet or contact key sponsors as 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.
10.4 Maintain adequate records of transactions	The MLRO will maintain a Register of all Report Forms. All disclosure reports and relevant documents will be retained in a confidential file for a minimum of six years. Departments conducting relevant transactions must maintain records for at least six years of Student / Customer identification evidence, and details of financial transactions carried out.

10.5 **Additional steps**

In addition, the University has implemented effective policies and controls to prevent and detect illegal activity by:

- carrying out regular risk assessments to identify activities and areas of operation most vulnerable to money laundering;
- undertaking appropriate staff awareness and training;
- enacting due diligence checks not only on the identity of customers, but also the accuracy of identifying information;
  implementing strong internal controls, to prevent and detect illegal activity, and learn from any incidents in order to improve internal controls further.

11. Monitoring and Review

11.1 This policy and related procedures will be reviewed annually by the Director of Finance & Commercial Development, the University Secretary and the Audit Committee. Risk identification (5 above) will form a key element of the overall monitoring and review process. Any incidents of money laundering reported to, and recorded by, the University Secretary will be incorporated into that review.

12. Associated Policies

12.1 The following policies are also available on the University Intranet

- Counter Fraud Policy
- Anti Bribery & Corruption Policy (including Gifts & Hospitality)
- Public Interest Disclosure Policy (‘’Whistleblowing’’)
- Criminal Finances Act Policy

13. What the University expects staff to do

13.1 Money laundering legislation applies to ALL employees. Potentially any member of staff could be committing an offence under the money laundering laws if they suspect money laundering or if they become involved in some way and do nothing about it.

13.2 Training and communication

13.2.1 The University will ensure that new members of the finance team receive appropriate anti-money laundering training as part of their induction. Each member of FCD staff will be required, annually, via MyCompliance, to verify that they have read and understood this policy. Refresher training will take place at each revision of the policy, at which point all staff will be asked to update their signed record. The University also subscribes to the training available from British Universities Finance Directors Group website.

13.2.2 This policy will be drawn to the attention of other University staff involved in student ID and finance checks at enrolment. These staff will be updated as necessary when the policy is revised.

13.2.3 This policy is published on the University’s intranet under Financial Regulations and is communicated to staff via internal communication, such as Update and MyCompliance.

13.3 Handling the proceeds of crime

All staff must avoid handling any money, goods or other items known or suspected to be associated with the proceeds of crime, or becoming involved with any services known or suspected to be associated with the proceeds of crime.

13.4 Reporting requirement

If any individual suspects that money laundering activity is or has taken place, or if any person becomes concerned about their involvement, it must be disclosed as soon as possible to the MLRO in accordance with the procedure contained in this policy below.

13.5 Cooperating with investigations

The individual must then co-operate fully with any investigations into reported

concerns. They must maintain confidentiality about any suspected or actual incidents involving the University. They should not make further enquiries into the situation or discuss their concerns with anyone else at any time, unless instructed by the MLRO. This is to avoid committing the offence of “tipping off” those who may be involved.

Failure to report money laundering concerns or "tipping off" anyone who may be involved in the situation may result in the member of staff being personally liable to prosecution under the 2017 Regulations.

14. How to report a concern

14.1 If a person suspects money laundering activity or becomes concerned about their involvement then they should:

- use the Money Laundering Report Form at the end of this policy (Appendix 3) to report the concern, giving as much information as possible, in writing, and without delay;

- send the Report Form as soon as possible to the University’s Money Laundering Reporting Officer (MLRO), marking the envelope “Confidential”;

- Remember not to make further enquiries into the situation or discuss their concerns with anyone else at any time, unless instructed by the MLRO. This is to avoid committing the offence of “tipping off” those who may be involved.

15. What the university will do in response

15.1 MLRO response

Upon receipt of a completed Money Laundering Report Form, the MLRO will complete the Response form. Consideration will be given to all relevant information, including:

- reviewing other relevant transaction patterns and volumes, and the length of any business relationship involved;
- reviewing the number of any one-off transactions, linked one-off transactions, and any identification evidence held;
- advising the reporter of the timescale within which a response can be expected.

15.2 MLRO inquiries

The MLRO will make other reasonable inquiries as appropriate in order to ensure that all available information is considered when deciding whether a report to the NCA is required. Inquiries will be made in such a way as to avoid any appearance of tipping off those involved.

15.3 Reporting to NCA

If the MLRO suspects money laundering or terrorist financing they will normally suspend the transaction and make a SAR to the NCA. However, a judgment will

be made regarding how safe and practical it is to suspend the transaction without "tipping off" the suspect. It may be necessary to make the report as soon as possible after the transaction is completed.

15.4 Maintaining a register

The MLRO will keep a separate Register of money laundering Report Forms and will update this Register with any relevant documents, including a copy of any SARs made to NCA and other NCA correspondence. These Report Forms and associated documentation should be kept for at least six years.

15.5 Disciplinary procedures

The University may follow disciplinary procedures against any member of staff who has committed a money laundering offence, which could result in dismissal.

15.6 References

Any request for a reference for a member of staff who has been disciplined or prosecuted for money laundering shall in all cases be referred to the Executive Director of Human Resources, who will respond having regard to employment law.

15.7 Reporting to the Office for Students

The MLRO should have regard to OfS's guidance on the reporting of "reportable events" in order to establish whether suspected or actual money laundering should be reported to them.

Risk	Description of risk	Risk mitigation/control	Risk assessment
Product/Service	The University offers instalment options to students for the payment of tuition and accommodation fees. The money laundering risks arise from these payment arrangements where the payment of funds come from unknown and/or unverified third parties	Most risks are mitigated as a result of the funds being paid direct to the university as the course provider by the student. Third-party payments are only accepted under limited circumstances, such as where the third-parties have been authorised by the student and are closely related to the student. However, additional electronic due diligence checks (e.g. credit checks) are performed where the third-party is unrelated e.g. sponsors.	Minor
Jurisdiction	The current jurisdiction for the University covers both UK and overseas activities, with some of those activities being undertaken in potentially higher-risk locations	All activities with overseas partners are subject to rigorous due diligence procedures. The University's Bank Transfer and Online Payment (outward) Platform is administered by Western Union Business Solutions (WUBS). WUBS complete compliance checks for incoming payments to the University and request additional information when transacting with higher-risk locations.	Minor

Customer/partner/third party	Most of the University's customers are UK residents, however a significant number of students will come from and/or study in overseas potentially higher risk locations. In addition the University may partner with overseas organisations during research activities or trans national education courses	Customer and partner due diligence procedures have been implemented to mitigate the potential customer risk: a) All new students have to present themselves at their School before they are made 'current' on the University's systems b) Creditsafe checks are undertaken in respect of Sponsors and partners (Home and overseas) c) Overseas sponsors are reviewed on the internet to ensure that they are bona fide d) Other individuals and organisations e.g. overseas agents and partners are subject to scrutiny and sign legally binding agreements e) We do not accept cash payments in excess of £2,500 f) Refunds are made to the original payer of the money	Minor
Distribution	The University faces a number of risks associated with how we undertake business, particularly where it is at a distance or online.	Business relationships with International Agents and partner institutions are only confirmed once the University has followed due process. Online and distance learning students must complete an application process which includes submission of previous qualifications and proof of identity	Minor

CUSTOMER DUE DILIGENCE (CDD) PRINCIPLES Appendix 2

Our customer due diligence follows the principles of Know Your Customer (KYC). The three components of KYC are:

1. Ascertaining and verifying the identity of the customer/student i.e. knowing who they are and confirming that their identity is valid by obtaining documents or other information from sources which are independent and reliable. In order to satisfy the requirements, identity checks for money laundering purposes are interpreted as obtaining a copy of photo-identification (such as a passport) and proof of address (such as a recent utility bill).

2. Ascertaining and verifying (if appropriate) the identity of the beneficial owners of a business, if there are any, so that you know the identity of the ultimate owners or controllers of the business.

3. Information on the purpose and intended nature of the business relationship i.e. knowing what you are going to do with/for them and why.

There are three levels of CDD - 'Standard', 'Simplified', and 'Enhanced'. 'Standard due diligence', as outlined above, should be applied to all financial relationships unless 'simplified' due diligence is or 'enhanced' due diligence is appropriate.

Simplified CDD does not require verification of the customer's identity and is appropriate when a risk assessment has shown a negligible or low risk of money laundering.

Enhanced CDD must be applied when the risk of money laundering is high, such as if the person in question is a politically exposed person (PEP). Enhanced due diligence measures may include:

- Additional identification information from the customer
- Information on the source of funds or source of wealth
- The intended nature of the business relationship
- The purpose of the transaction
- Subjecting the customer to additional ongoing monitoring procedures

Appendix 3

CONFIDENTIAL - Suspected Money Laundering Reporting Form *Please complete and send this (in a physical format) to the MLRO using the details below*	
From:	School/Service:
Contact Details :	
DETAILS OF SUSPECTED OFFENCE [Please continue on a separate sheet if necessary]	
Name(s) and address(es) of person(s) involved, including relationship with the University:	
Nature, value and timing of activity involved:	
Nature of suspicions regarding such activity:	
Details of any enquiries you may have undertaken to date:	
Have you discussed you suspicions with anyone? And if so, on what basis?	
Is any aspect of the transaction(s) outstanding and requiring consent to progress?	
Any other relevant information that may be useful?	
Signed:	Date:
Please do not discuss the content of this report with anyone you believe to be involved in the suspected money laundering activity described. To do so may constitute a tipping off offence, which carries a maximum penalty of 5 years' imprisonment and/or an unlimited fine.	

MLRO Report (to be completed by MLRO only)			
Date report received: / /	Date receipt of report acknowledged: / /		
Consideration of Disclosure: [Please continue on a separate sheet if necessary]			
Action plan:			
Outcome of consideration of Disclosure:			
Are there reasonable grounds for suspecting money laundering activity?			YES/NO
If there are reasonable grounds for suspicion, will a report be made to the NCA?			YES/NO
If yes, please record the date of report to NCA and complete the details below: Date of report: / / Details of liaison with the NCA regarding the report: Notice Period: …….. to …….. Moratorium Period: …….. to ……			
Is consent required from the NCA to any ongoing or imminent transactions that would otherwise be prohibited acts? If yes, please confirm full details below:			YES/NO
Date consent received from NCA:			/ /
Date consent given by you to employee:			/ /
If there are reasonable grounds to suspect money laundering, but you do not intend to report the matter to the NCA, please set out below the reason(s) for non-disclosure:			
Date consent given by you to employee for any prohibited act transactions to proceed:			/ /
Signed		Date:	/ /
THIS REPORT TO BE RETAINED FOR AT LEAST FIVE YEARS			