ANTI-MONEY LAUNDERING (AML) POLICY

1. Introduction

1.1 The University is 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 This Policy applies to:

- all University staff and Governors; and
- all University activities undertaken in the UK or overseas

1.3 The University will not tolerate money laundering activity, carried out by its own staff or by third parties involved with the University's activities and encourages its staff, contractors and related parties to report concerns and suspicious activity.

1.4 The University is committed to high standards of ethical behaviour and preventing and detecting all criminal activity, including money laundering. It is no longer acceptable to conduct business on trust alone.

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

2.2 There are three stages in money laundering; placement, layering and integration.

- Placement– the process of getting criminal money into the financial system;
- Layering – the process of moving the money within the financial system through layers of transactions; and
- Integration – the process whereby the money is finally integrated into the economy, perhaps in the form of a payment for a legitimate service.

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

- the principal money laundering offences under the Proceeds of Crime Act 2002;

- the prejudicing investigations offence under the Proceeds of Crime Act 2002; and

- offences of failing to meet the standards required of certain regulated businesses, including offences of failing to disclose suspicions of money laundering and failing to comply with the administrative requirements of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.

3. Responsibilities and Expectations

3.1 Responsibilities

3.2 The Chief Financial Officer, as the Nominated Officer, is responsible for implementing and maintaining anti-money laundering procedures and responding to reports of suspected money laundering activity. In the absence of the Chief Financial Officer, the Assistant Director (Financial Accounting) will act as the Nominated Officer.

3.3 The Nominated Officer is responsible for:

- receiving reports of suspicious activity from any employee in the business and maintaining a Register of all Report Forms;

- considering all reports and evaluating whether there is - or seems to be - any evidence of money laundering or terrorist financing;

- reporting any suspicious activity or transaction to the National Crime Agency (NCA) by completing and submitting a Suspicious Activity Report

- asking NCA for consent to continue with any transactions that they have reported and making sure that no transactions are continued illegally

3.4 Expectations of University staff

General expectations of university staff include:

- to discharge their duties in accordance with their contractual obligations and with due regard to University policies and procedures;

- to 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

- to remain vigilant and report concerns related to suspected money laundering activity

- to co-operate fully with any investigations into reported concerns

- to maintain confidentiality about any suspected or actual incidents involving the University

4. Principal Money Laundering Offences

4.1 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:

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

4.2 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.

4.3 In all three cases, there is a defence if a so-called *authorised disclosure* of the transaction is made either to the Nominated Officer or to National Crime Agency and the National Crime Agency does not refuse consent to it.

4.4 It is a crime, punishable by up to five years imprisonment, 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.

4.5 At section 6.7 below, this policy sets out how such disclosures are to be made.

4.6 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. This policy requires that all authorised disclosures to be kept strictly confidential.

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

4.7.1 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. 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, punishable by up to 14 years imprisonment, of:

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

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, 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 6.7 below.

5.7 The Offence of Prejudicing Investigations

5.7.1 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 paragraph 35 below, this policy requires disclosures under the Terrorism Act 2000 to be kept strictly confidential.

6. University Procedures

6.1 The University adopts a risk-based approach towards anti-money laundering and conducting due diligence. Whilst much of the University's financial activities could be considered relatively low risk from the prospective of money laundering, all staff need to be vigilant against the financial crime and fraud risks that the University faces.

6.2 The University is required to undertake an annual risk assessment. There are four main risks areas to review, these are listed in Appendix A along with examples of suspicious activity. The risk assessment report is included at Appendix B and includes risks specific to the University and the controls in place to mitigate against these risks.

6.3 The University has appointed a Nominated Officer to whom concerns should be reported and who will report any suspicious transactions to the National Crime Agency

6.4 Customer Due Diligence

6.4.1 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 B which will be reviewed annually.

6.4.2 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:

- ascertaining and verifying the identity of the customer/student and confirming this by obtaining documentary evidence (photocopy of photographic identification and proof of address)
- ascertaining and verifying (if appropriate) the identity of the beneficial owners of a business
- details of the purpose and intended nature of the business relationship

6.5 In addition to a check on customers, the University must also undertake due diligence on transactions including:

- identifying and verifying the identity of a payer or a payee, typically a student or a donor;
- where the payment is to come from or to be made by a third party on behalf of the student or donor, identifying and verifying the identity of that third party;
- identifying and verifying the source of funds from which any payment to the

University will be made; and

- identifying and in some circumstances verifying the source of wealth from which the funds are derived.

Source of funds refers to where the funds in question are received from. The most common example of a source of funds is a bank account. Source of wealth refers to how the person making the payment came to have the funds in question. An example of a source of wealth is savings from employment.

6.6 Sanctions

6.6.1 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.

6.6.2 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-consolidatedlist-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.

6.7 Reporting

6.7.1 Having completed the due diligence exercise, we can now assess the money laundering and terrorist finance risk associated with the transaction by referring to the flow chart included in Appendix C.

6.7.2 Where you know or suspect that money laundering activity is taking place, or has taken place, or you are concerned that a transaction may be in breach of regulations, you must notify the Nominated Officer as soon as is practicable using the form in Appendix D.

6.7.3 Avoiding the criminal offence of "tipping off". Once reported, staff should make no further enquiries into the situation or discuss their concerns with anyone else at any time, unless instructed by the Nominated Officer. Neither should they make any reference on a file to a report having been made. The appropriate records will be kept in a confidential manner in by the Nominated Officer. Following this advice will protect employees from committing the criminal offence of "tipping off".

6.8 Record Keeping

6.8.1 The University retains records for five years after ceasing to transact with a customer including records of customer risk assessment, customer identity and verification and customer ongoing monitoring.

7. University Actions

7.1 Upon receipt of a completed Money Laundering Report Form (Part 1), the Nominated Officer must complete Part 2 of the form. Consideration will be given to all relevant information, including:

- reviewing other relevant transaction patterns and volumes; the length of any business relationship involved
- the number of any one-off transactions and linked one-off transactions; any identification evidence held

7.2 The person making the report will be advised of the timescale within which a response can be expected.

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

7.4 If the Nominated Officer or nominee suspects money laundering or terrorist financing they will normally suspend the transaction and make a Suspicious Activity Report to SOCA. However, a judgment should 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.

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

7.6 The Nominated Officer or nominee will keep a separate Register of money laundering Report Forms and will update this Register with any relevant documents, including a copy of any "Suspicious Activity Reports" made to SOCA and other SOCA correspondence.

7.7 The Chief Financial Officer will devise and implement arrangements to ensure that compliance with this policy is kept under continuous review through regular file reviews, including reviews of due diligence and risk assessment, and reports and feedback from staff. Internal audit may be called upon to assist in monitoring effective implementation of this policy.

7.8 To enable monitoring to be conducted and compliance with this policy to be evidenced, the University will retain all anti-money laundering and counter-terrorist finance records securely for a period of at least five years.

7.9 Training

7.9.1 On joining the University any staff whose duties will include undertaking a finance function will receive anti-money laundering training as part of their induction process.

7.9.2 All staff undertaking a finance function will receive annual refresher anti-money laundering and counter-terrorist finance training.

7.9.3 The University's anti-money laundering and counter-terrorist financing training will include the applicable law, the operation of this policy and the circumstances in which suspicions might arise.

8. Other Actions

8.1 In order to minimise the potential for money laundering activities the University has developed the following procedures.

8.2 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 for accommodation or tuition fees and to where possible not accept cash payments for any goods or services.

8.3 Requests for Refunds

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

8.4 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.

8.5 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.

Appendix A – Risk Areas and Examples of Potential Money Laundering Activity

Risk Areas	
Jurisdiction Risk	Risks associated with transacting with certain locations and jurisdictions.
Customer/3rd Party Risk	Most of the University's customer are residents in the UK or EEA countries. However some customers will come from/study overseas in potentially higher-risk locations. In addition, the University may partner with overseas organisations for teaching and research purposes.
Distribution Risk	Risks associated with how the University undertakes business, particularly off campus, for example on-line activities or indirect relationships via agents or 3rd party representatives.
Product/Service Risk.	Many of the University's operations do not present an opportunity for money laundering, however there are risks around acceptance of funds and processing refunds.

The examples below are not intended to be exhaustive but provide a general indication of the range of matters covered by this Policy.

Money laundering: Examples of suspicious activity
Payment by a person or company of any substantial sum in cash (over £10,000), particularly if they fail to provide proper evidence to confirm their identity and address.
A person or company doing business with the University lacks proper paperwork, e.g. invoices that exclude VAT, failure to quote a VAT number or invoices issued by a limited company that lack the company's registered office and number.
A person or company attempts to engage in circular transactions, where a payment to the University is followed by an attempt to obtain a refund from the University's accounts. (This may occur where a student pays a significant sum in fees, and then withdraws and seeks a refund).
Unusual or unexpected large payments are made into the University's accounts.
A secretive person or business e.g. that refuses to provide requested information without a reasonable explanation.
Students requesting a large cash transaction, particularly where the cash is used notes or small denominations.
Absence of any legitimate source for funds received
Overpayments for no apparent reason.
Involvement of an unconnected third party without a logical reason or explanation. Significant changes in the size, nature, frequency of transactions with a customer that is without reasonable explanation.
Requests for payments or refunds after funds have been paid into the University's bank account by a third party, particularly if there is a request to return money to a different account or individual to the payer.
Cancellation, reversal or requests for refunds of earlier transactions

Appendix B

Annual Anti-Money Laundering Risk Assessment

1. Introduction

1.1. The University has undertaken a risk assessment of our current operations in order to review our policies and procedures to ensure that these are deemed proportional to the potential money-laundering crime risks that we face.

2. Risk Areas & Mitigating Actions

2.1. Jurisdiction/Distribution Risks

The University recognises that there are additional risks associated with transactions in certain locations including the University's countries of operation, location of customers, suppliers and agents. In addition, there are countries that are known to have inadequate anti-money laundering (AML) controls, those that are subject to sanctions, embargoes and countries identified as supporting terrorism.

- we will monitor relevant websites to identify such countries
- undertake customer due diligence
- bank transfer and on-line payments

2.2. Customer Risk

There is no definitive list of behaviours that may indicate suspected money laundering activity or how to decide to make a report to the Nominated Officer, however the following behaviours/activities may be indications of risks of potential money-laundering activities that should be considered:

- new customers or partners that are not currently known to the University – customer due diligence should be undertaken to mitigate this risk
- customers who refuse to provide information requested without a reasonable explanation
- payments of substantial amounts of cash – University policy is not to accept cash payments for outstanding debt
- concerns about the honesty, integrity or location of individuals or absence of a legitimate source of funds
- involvement of an unconnected 3rd party without a logical explanation
- overpayments for no reason, especially when refunds are requested via an alternative payment method/to another party
    - refunds are paid to the same source as the original payment
    - refunds must be made with appropriate authorisation
- significant changes in transactions with a customer without explanation
- other suspicious requests or activity

2.3. Products/Services Risk

The risks associated with the products and services offered by the University are reasonably low and will be covered by Know Your Customer processes and controls over income receipts. The main risks are:

- Students
    - students are required to register via our e-registration process including passport and visa checks are appropriate
    - we do not accept cash payments for outstanding debts
    - refunds must be properly authorised and are paid to the original source of the receipt

- Procurement
    - The University is committed to contracting only with suppliers and contractors that comply with all relevant legislation. Further details are available within our various procurement policies and procedures

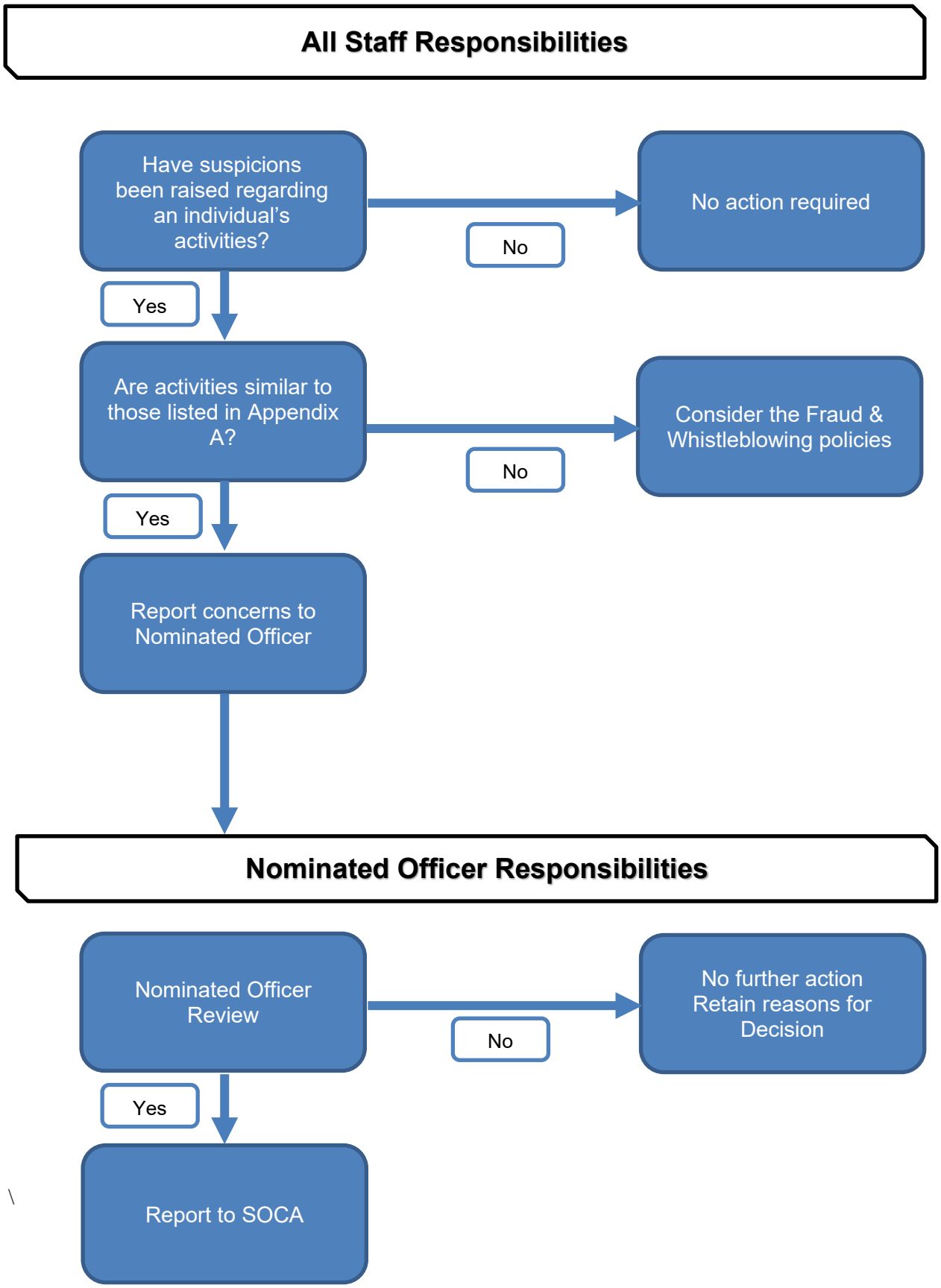
- Research
    - The University has a wide ranging Research Governance Handbook covering all aspects of research including collaborations, partnerships, activity and research ethics. There are additional due diligence procedures in place to comply with Overseas Development Assistance requirements as part of Research Funders terms and conditions.

- Endowment & Donations
    - The University will undertake all necessary checks before accepting donations etc. from any source.

3. Relevant Polices & Procedures

- Financial Regulations
- Criminal Finances Act Statement
- Ethical Statement
- Fraud Policy
- Whistleblowing
- Credit Policy
- Infohub - does not accept cash payments
- Research Governance Handbook
- Student Admissions Guidance

Appendix C – Reporting Money Laundering Concerns
(accessible version on next page)



Appendix C – Reporting Money Laundering Concerns (accessible version)

This procedure consists of 3 steps:

All Staff Responsibilities

1. If no suspicions have been raised regarding an individual's activities, then no action is required.
2. Where suspicions been raised regarding an individual's activities, check to see if the activities are similar to those listed in Appendix A
    - If they are similar, then report concerns to the Nominated Officer
    - If they are different, then consider implementing the Fraud and Whistleblowing policies

Nominated Officer Responsibilities

3. The Nominated Officer reviews the concerns and reports to SOCA if further action is required. If no further action is required, the reasons for the decision are to be retained

Appendix D

CONFIDENTIAL SUSPECTED MONEY LAUNDERING REPORT	
From:	**School/Directorate:**
Contact Details:	
DETAILS OF SUSPECTED ACTIVITIES:	
Names and addresses of persons involved (including relationship with the University)	
Nature, value and timing of the activities:	
Nature of suspicions:	
Please provide details of any investigation undertaken to date:	
Have you discussed your 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.	

PART 2 - NOMINATED OFFICER Report	
Date report received:	**Date of report acknowledgement:**
Review of Initial Report:	
Actions arising:	
Are there reasonable grounds for suspicion of money laundering activates?	**YES/NO**
If Yes, will a report be prepared for the SOCA?	**YES/NO**
Details of SOCA Report (if applicable) **Date Sent:** **Summary of Report:**	
Is consent required from the SOCA to any ongoing or imminent transactions which would otherwise be prohibited acts? <u>If yes</u>, please confirm full details below:	
Is consent required from the SOCA to any ongoing or imminent transactions which would otherwise be prohibited acts? **Please confirm full details below (if applicable):**	**YES/NO**
Details:	
Date consent received from SOCA:	
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 SOCA, please set out below the reason(s) for non- disclosure:	
Signed	**Date:**
PLEASE RETAIN FOR AT LEAST FIVE YEARS	