September 2019

1495 UNIVERSITY OF ABERDEEN

**ANTI-MONEY LAUNDERING (AML) POLICY**

## 1. Introduction

1.1. 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.

1.2. There are three stages in money laundering; placement, layering and integration. Placement is where the proceeds of criminal activity enter into the financial system; layering distances the money from its illegal source through layers of financial transactions; finally, integration involves the re-introduction of the illegal proceeds into legitimate commerce by providing an apparently-genuine explanation for the funds.

1.3. This Policy outlines how the University and its employees will manage money laundering risks and comply with its legal obligations under the following:

- Proceeds of Crime Act 2002 (as amended)
- Terrorism Act 2000 as amended by the Anti-terrorism, Crime and Security Act 2001)
- Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017)
- Counter-terrorism Act 2008, Schedule 7
- HM Treasury Sanctions Notices and News Releases
- Joint Money Laundering Steering Group (JMLSG) Guidance

1.4. MLR2017 replaces MLR2007 and adopts a more risk-based approach to AML and due diligence. MLR2017 is more prescriptive, particularly in relation to risk mitigation.

## 2. Approach to Money Laundering

2.1. 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.

2.2. This Policy applies to:

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

2.3. 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. Instances of suspected money laundering are likely to be rare at the University but we must be aware of legislative requirements.

2.4. The University assesses risks relevant to our operations, and puts in place the processes and procedures that we deem necessary to mitigate these risks. We determine the appropriate level of due diligence by looking at the geographic and customer risk factors based on the EU Directive and

set out in MLR2017 and analysing the University's potential exposure to money laundering (the source of funds) or terrorist financing (the destination of funds).

2.5. 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.

2.6. The University has identified staff to whom concerns should be reported and who will refer concerns to the Serious Organised Crime Agency ("SOCA") if required.

2.7. This University has established an appropriate policy to minimise the risks in relation to money laundering. This policy constitutes the statement of commitment to the guiding principles and demonstrates the top level commitment as required by MLR2017.

- **Risk assessment and management**
  The University has appointed a nominated officer, the Money Laundering Reporting Officer (the "MLRO") as detailed in section 3.3. Assessments of money laundering risks in terms of the different operations, products and services provided and the respective customer bases, are made by the MLRO in liaison with appropriate line management. Further details of the different risks are provided in Appendix A. The University's AML risk report is attached in Appendix B.

- **Customer due diligence**
  As required by the MLR 2017, the University has policies and procedures for performing customer due diligence ("CDD"), and 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. 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, ascertain 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

- **Reporting**
  The University through the appointed Money Laundering Reporting Officer (MLRO) has established procedures for reporting and assessing internal suspicious activity and on the decision making process for external reporting. Staff should report concerns for investigation by the MLRO to determine whether there is knowledge or a suspicion of money laundering.

  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 disclose this immediately. The University, through the MLRO, will take all reasonable steps to identify and report suspicious transactions, of all types. This includes Sanctioned Parties (see next section).

- **Sanctions**
  Financial sanctions which relate to a specific country or terrorist group which are known as 'regimes'. What is prohibited under each financial sanction depends on the financial sanction regulation. Regulations are imposed by the:

  - United Nation's Security Council – the UK is a member so automatically imposes all financial sanctions created by the UN;
  - European Union – as a member of the EU, the UK imposes all financial sanctions created by the EU;
  - UK Government – a small number of financial sanctions are created by the UK Government.

  The University's MLRO will monitor the relevant websites to review Sanctioned Parties and ensure that the University does not transact with Sanctioned Parties.

- **Record Keeping**
  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.

## 3. Responsibilities and Expectations

### 3.1. Responsibilities

3.2. The Director of Finance, as the nominated Money Laundering Reporting Office (MLRO), is responsible for implementing and maintaining anti-money laundering procedures and responding to reports of suspected money laundering activity. In the absence of the Director of Finance, the Assistant Director (Financial Accounting) will act as MLRO.

3.3. The MLRO 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 SOCA (Serious Organised Crime Agency) by completing and submitting a Suspicious Activity Report
- asking SOCA 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

3.5. Staff are reminded that money laundering legislation applies to ALL employees. Staff could be committing an offence if they suspect money laundering (or if they become involved in some way) and do nothing about it. Examples of warning signs of potential money laundering activities are shown in Appendix A.

3.6. If a member of staff suspects that money laundering activity is taking or has taken place or if any person becomes concerned about their involvement then staff should follow the reporting process outlined in Section 5.

3.7. Once reported, staff 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.

3.8. 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 2007 Regulations.

## 4. Reporting concerns about suspected Money Laundering

4.1. Money laundering legislation requires concerns to be reported in writing as outlined below. All actual or suspected instances of irregularity relating to the scope of this Policy should be reported without delay - see Appendix C for a flowchart of the reporting channels for raising concerns.

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

- use the Money Laundering Report Form at Appendix D to report the concern, giving as much information as possible
- send the Report Form as soon as possible to the Finance Director, who acts as the University's Money Laundering Reporting Officer (MLRO)

4.3. **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 MLRO. 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 MLRO. Following this advice will protect employees from committing the criminal offence of "tipping off".

## 5. University Actions

5.1. Upon receipt of a completed Money Laundering Report Form (Part 1), the MLRO 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

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

5.3. 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 SOCA is required. Inquiries will be made in such a way as to avoid any appearance of tipping off those involved.

5.4. If the MLRO 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.

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

5.6. 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 “Suspicious Activity Reports” made to SOCA and other SOCA correspondence.

5.7. Current SOCA guidance requires that Report Forms and associated documentation should be kept for at least five years.

**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 MLRO, 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

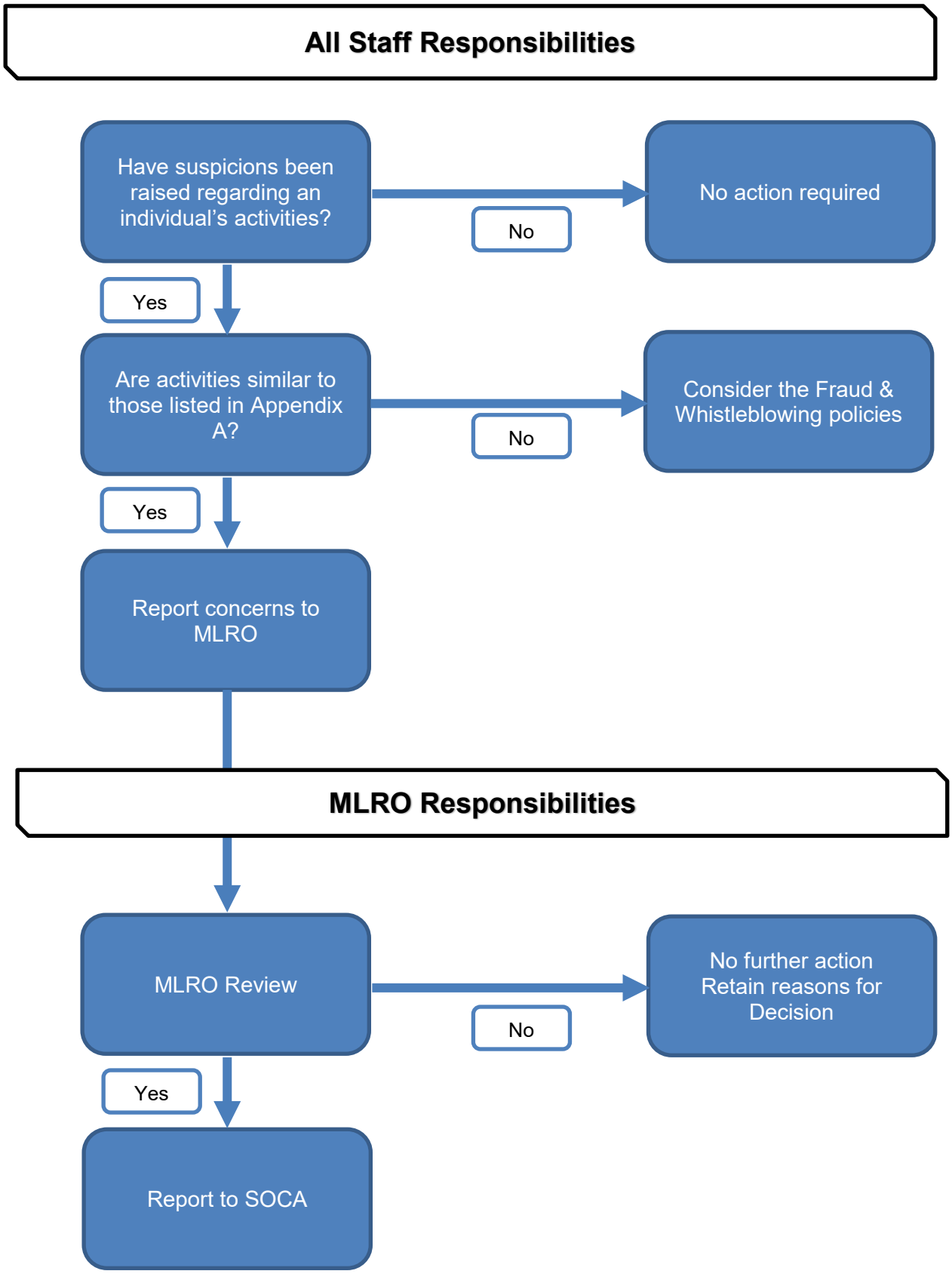
- Research
    - The University has a wide ranging Research Governance Handbook covering all aspects of research including collaborations, partnerships, activity and research ethics. There are additional due diligence procedures in place to comply with Overseas Development Assistance requirements as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



## Appendix D

| **CONFIDENTIAL SUSPECTED MONEY LAUNDERING REPORT**<br><br>**PART 1 - REPORT TO MLRO** | |
|---|---|
| **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 - MLRO 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)**<br><br>**Date Sent:**<br><br>**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?**<br><br>**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** | |