

# Anti-Money Laundering Policy

## INTRODUCTION

### 1.1 Purpose of Policy

The University of Bath is committed to ethical standards of business conduct and adopts a zero-tolerance approach to financial misconduct, including money laundering. The University will uphold legislation for countering money laundering, including, The Proceeds of Crime Act 2002 (as amended by the Crime and Courts Act 2013 and the Serious Crime Act 2015), the Terrorism Act 2000 (as amended by the Anti-Terrorism, Crime and Security Act 2001), Counter-Terrorism Act 2008 Schedule 7, and the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, HM Treasury Sanctions Notices and News Releases, now incorporated in the Money Laundering Regulations 2017 and the Criminal Finances Act 2017.

The purpose of this policy is to outline how the University and its staff will manage money laundering risks, apply 'Know your Customer' principles and comply with the relevant legislation.

### 1.2 Scope

- 1.2.1 This policy applies to all members of University staff, including students acting as employees of the University, and associated parties, including members of Council, and covers University activities undertaken in the UK or overseas. Money laundering legislation applies to all employees of the University.
- 1.2.2 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. 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 University's Money Laundering Reporting Officer (MLRO), as outlined in Section 2.3 below.
- 1.2.3 Breach of this Policy may constitute a disciplinary offence for staff and will be subject to investigation under the University's disciplinary procedures. This may lead to disciplinary action, including dismissal. Failure to comply with this Policy may expose staff to the risk of being personally liable to prosecution.
- 1.2.4 Non-compliance with this legislation carries financial and reputational penalties for both the University and its staff. Whilst the risk to the University of contravening the legislation is considered to be low, it is extremely important that all staff are familiar with their legal responsibilities as serious criminal sanctions may be imposed for breaches. The key requirement on employees is to promptly report any suspected money laundering activity to the Money Laundering Reporting Officer (MLRO).

## 2. POLICY

### 2.1 What is money laundering?

2.1.1 Money laundering is the process of taking the proceeds of criminal activity and making them appear legal. It can also encompass financial transactions involving money, however obtained, which is used to fund terrorism. The definition of money laundering activities under the legislation referenced above is broad.

2.1.2 There are three principal money laundering offences under the Proceeds of Crime Act 2002:

- concealing, disguising, converting, transferring criminal property or removing it from the UK (section 327 of the 2002 Act); or
- entering into or becoming concerned in an arrangement which you know, or suspect facilitates the acquisition, retention use or control of criminal property by or on behalf of another person (Section 328); or
- acquiring, using or possessing criminal property (section 329)

2.1.3 These offences can be punishable by unlimited fines and/or terms of imprisonment up to a maximum of 14 years.

2.1.4 There are also associated offences regarding due diligence and disclosures, including:

- Failure to disclose any of the three primary offences;
- Failure to have adequate procedures for mitigating the risk of money laundering;
- Tipping off. Tipping off is where someone informs a person or people who are, or who are suspected of being involved on money laundering in such a way as to reduce the likelihood of their being investigated or prejudicing and investigation.

### 2.2 What steps can we take to prevent money laundering?

2.2.1 We can take the following steps to assist in the prevention of money laundering:

- **Maintain adequate records of transactions** Departments conducting relevant transactions must maintain records for at least six years of:
  - Student/Customer identification evidence
  - Details of financial transactions carried out.

In practice each area will routinely create and retain records in the course of normal business, and these will be sufficient for this purpose.

- **Implement a procedure to enable the reporting of suspicious activity;** The legislation requires the University to disclose when it has actual knowledge or suspicion of money laundering but also if, given the circumstances, it should have reached that conclusion and failed to do so. We should be familiar with the type of customer who normally approaches us for business, and how they normally deal with us. Suspicion may be

aroused if a customer deals with us differently to our normal experience or wants things that are out of the ordinary for the type of business concerned. If suspicion is aroused members of staff should forward their concern to the MLRO immediately. Examples of suspicious activity are given in Appendix 1.

- Implement customer identification or ‘know your customer’ procedures;** When taking orders for business from customers in respect of work that counts as ‘relevant business’ staff must be reasonably satisfied as to the identity of the customer that they are engaging with. It is important that due diligence controls are in place to identify the student, customer or other party dealing with the University. Satisfactory evidence of identity must be obtained. Examples include passport, visa and birth certificate, correspondence with students at their home address and for third parties, letters or documents proving name, address and relationship. If an organisation is not known to the University look for letter-headed documents, check websites, 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 regarding validity of the source.
- Maintain an Anti-Money Laundering Risk Assessment** The Standing Group on Financial Probity will maintain the University’s Anti-Money Laundering Risk Assessment, reviewing it on an annual policy and making recommendations as appropriate to the University’s Executive Board. The Money Laundering Regulations 2017 require the university to undertake a risk assessment, encompassing four key areas of risk which must be considered in assessing the overall risk level.

**Product/Service Risk** - This is the risk associated with the delivery of University activity, including teaching, research, knowledge exchange, fundraising and events & conferencing.

**Jurisdiction Risk** – This is the risk associated with the geographical reach of the University’s activities, including the countries in which its international students, strategic academic partners, alumni and donors, agents and suppliers are based.

**Customer, Third Party/Donor Risk** – This is the risk associated with the individuals and/or third party organisations with whom we do business, including our customers, academic partners, contractors, agents and suppliers. Politically Exposed Persons and Sanctioned Parties are also considered within this risk.

**Distribution Risk** – This is the risk associated with how we deliver our products and services, including in-person, digital/online and telephony.



- Ensure adequate **training** is given to staff on anti-money laundering procedures and policies, including how to report/disclose suspicious activity. The University has identified the following departments as being at higher risk of encountering money laundering activities and will ensure that they receive appropriate training:

- Finance & Procurement Office;

- Development and Alumni Relations;

- Corporate Engagement.

All members of these teams will be required to read the Policy on an annual basis and confirm to the Standing Group on Financial Probity that they have done so.

- **Appoint a Money Laundering Reporting Officer to develop and maintain the University's anti-money laundering procedures and receive, consider and report**, as appropriate, on any disclosure of suspicious activities by staff. The University has appointed Mr Martin Williams, Director of Finance, as its Money Laundering Reporting Officer - [mw314@bath.ac.uk](mailto:mw314@bath.ac.uk).

## 2.3 How do you report suspicious activities?

2.3.1 Where you know or suspect that money laundering activity is taking or has taken place, or you become concerned that your involvement in a transaction may amount to a breach of this Policy and money laundering regulations, you must disclose this immediately to your line manager. If in consultation with your line manager reasonable suspicion is confirmed a disclosure report must be made to the MLRO.

2.3.2 This disclosure should be made on the proforma report attached in Appendix 3 and should be completed the same day the information comes to your attention. Should you not do so you may be personally liable to prosecution under the money laundering regulations.

2.3.3 Your report should include as much detail as possible including:

- Full available details of the people, companies involved including yourself and other members of staff if relevant
- Full details of transaction and nature of each person's involvement in the transaction Suspected type of money laundering activity or use of proceeds of crime with exact reasons as to why you are suspicious
- The dates of any transactions, where they were undertaken, how they were undertaken, and the likely amount of money or assets involved
- Any other relevant information.

2.3.4 Upon receipt of a disclosure report, the MLRO must note the date of receipt and acknowledge receipt of the report. The MLRO will advise you of the timescale within which they will respond.

2.3.5 To avoid committing the offence of tipping off, once you have submitted the disclosure form you should not make any further enquiries into the situation, nor should you discuss your concerns with others unless instructed to do so by the MLRO.

### 3. ROLES AND RESPONSIBILITIES

- 3.1 Any member of staff or associated party who suspects that money laundering activity is or has taken place or becomes concerned about their involvement in a transaction must disclose this, in writing, as soon as possible to the University's Money Laundering Reporting Officer (MLRO), as outlined in section 2.3 above. Individuals must then co-operate fully with any subsequent investigations whilst maintaining confidentiality about the suspected activity.
- 3.2 The Money Laundering Reporting Officer is responsible for developing and maintaining appropriate anti-money laundering procedures and for receiving, considering and reporting, as appropriate, on any disclosure of suspicious activities by staff. The MLRO will investigate all reports or disclosures in accordance with the procedure outlined in Appendix 3. The MLRO will be responsible for suspending a transaction and making a Suspicious Activity Report to the National Crime Agency, if there is a suspicion of terrorist financing or money laundering. The MLRO is responsible for maintaining a Register of Disclosure Forms and Suspicious Activity Reports.
- 3.3 The Director of Policy, Planning and Compliance will be responsible for ensuring that a 'Reportable Event' report is submitted to the Office for Students, if appropriate, in line with the University's ongoing conditions of registration obligations.
- 3.4 The Standing Group on Financial Probity will be responsible for undertaking an annual review of the University's Anti-Money Laundering Risk Assessment (Appendix 4) and for ensuring that the Policy is reviewed on a three-year cycle, or as new legislation prompts a review.

### 4. RELATED POLICIES AND PROCEDURES

University of Bath Financial Regulations:

<http://www.bath.ac.uk/finance-procurement/regulations-policies-procedures/index.html>

Public Interest Disclosure Policy (Whistleblowing Policy):

<http://www.bath.ac.uk/university-secretary/pdf/public-interest-disclosure.pdf>

Risk Management Strategy:

<https://www.bath.ac.uk/corporate-information/risk-management-strategy/>

### 5. DOCUMENT CONTROL INFORMATION

Owner	Director of Finance
Version number	New Policy Framework, Version 1
Approval Date	26 November 2020
Approved By	Council
Date of last review	Not applicable
Date of next review	2023

### ANTI-MONEY LAUNDERING GUIDANCE

#### Examples of Risk Areas

Instances of suspected money laundering are likely to be rare given the nature of services provided by the University. The following are examples of activities where colleagues should be alert to the risks of money laundering:

#### New Customers

- Is checking their identity proving difficult? Is the customer reluctant to provide details?
- Is there a genuine reason for using the services of the University or its subsidiary company?
- Is the customer trying to introduce intermediaries whether to protect their identity or hide their involvement?
- Is the customer requesting a large cash transaction – especially where cash is used notes and/or in small denominations?
- Is the customer requesting cash in large denomination notes?
- Is the source of the cash known and reasonable?
- Where transactions involve international transfers or foreign currency, is the explanation for the business and the amount involved reasonable?
- Are there any unusual requests for collection or delivery?
- Cancellation, reversal or requests for refunds of earlier transactions?
- Overpayments with no credible explanation?
- Does the customer lack proper paperwork, e.g. does the invoice exclude VAT or is it from a limited company but fails to quote a VAT number or the company's registered address and number?

#### Regular and Established Customers

- Is the transaction reasonable in the context of the normal business of this customer?
- Is the size and frequency of the transaction consistent with the normal activities of the customer?
- Has the pattern of transaction changed since the business relationship was established?

## APPENDIX 2

### Disclosure report

Internal reference number:

### Suspected Money Laundering - Report to the Money Laundering Reporting Officer (MLRO).

From: .....

Department: .....

Contact details: .....

#### DETAILS OF SUSPECTED OFFENCE

- Name(s) and date of Birth
- Address (es) of person(s) involved including postcode
- Relationship with the University.
- Nature, value and timing of activity involved.
- Disclosure type (nature of suspicions regarding such activity)
- 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 .....

## APPENDIX 3

### Procedure for the Investigation of Suspicious Activities

The MLRO will note and acknowledge any disclosure received and advise the individuals involved as to when a response can be expected. The MLRO will consider the report and any other available internal information they think are relevant e.g.

- 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.

The MLRO will then carry out further enquiries as necessary to investigate the matter. Inquiries will be carried out in such a way as to avoid the appearance of any tipping off of those involved.

The MLRO shall report all suspected incidents of money laundering to the competent authorities. Under the Proceeds of Crime Act, this requires a Suspicious Activity Report (SAR\_ to be forwarded to the National Crime Agency:

<http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/ukfiu/how-to-report-sars>

The MLRO shall use their discretion in deciding whether to suspend a transaction whilst any report to the competent authorities is made.

All disclosures and relevant documentation will be retained in a confidential file by the Director of Finance for a minimum of six years.

## APPENDIX 4

### Anti-Money Laundering Risk Assessment

Risk Area	Description of Risk	Risk mitigation/control
Products & Services	Cash transactions, anonymous transactions, transactions involving unknown third parties and unregulated transactions	<p>Most risks are mitigated as a result of the funds being paid direct to the University as the course or service provider.</p> <p>Third party payments are only accepted under limited circumstances, such as where the third parties have been authorised by a student and are closely related to the student.</p> <p>Additional due diligence checks are performed where the third party is unrelated.</p> <p>We recognise that there are AML risks associated with refunds and will raise the awareness of those involved in processing such transactions that constant vigilance is required.</p>
Customers, third parties and donors	<p>Whilst the majority of our students are UK residents, we recruit a significant proportion of international students some of which will come from/study in higher risk locations.</p> <p>The University conducts a significant amount of research in partnership with international partners, and is seeking to increase its international partnerships.</p> <p>The University has established a number of international chapters for its alumni base and hosts events in country.</p>	<p>Customer due diligence procedures are implemented to mitigate this risk:</p> <p>(a) All new students have to present proof of identity as part of our registration processes.</p> <p>(b) Refunds are made to the original payer of the money.</p> <p>(c) Creditsafe checks(?)</p> <p>(d) Overseas sponsors(?)</p> <p>(e) Maximum limit for cash payments(?)</p> <p>(f) anonymous payments not accepted.</p> <p>(g) DDAR review all potential and confirmed donations over £50,000 and verify the identity of the</p>

		donor checking it against known databases such as DDIQ (part of Exiger) and Company House records.
Jurisdiction	Our activities are conducted in the UK and overseas, with some of the overseas activities being undertaken in potentially higher-risk locations. In particular, we recognise that some countries do not have robust AML approaches, and some may be subject to sanctions or embargoes.	Activities with international partners are subject to due diligence procedures.  (WUBS?)  Creditsafe(?)
Distribution	Much of the University's teaching activity is delivered on its Claverton Campus and represents a low risk. However, the University has in recent years increased its provision of blended/online delivery which presents a higher level of risk. The University is also in the process of constructing a new research facility, IAAPS, which will offer services and products to a wide range of third parties.	Online and distance learning students must produce proof of identity and prior qualifications.  Business relationships with International Agents are governed by formal contracts.  MoUs and other academic partnerships are only confirmed after implementation of the appropriate procedures.

The University has assessed each of these risk areas on a RAG (Red, Amber, Green) scale equating to high, medium and low risk. All of these risk areas are currently assessed as Green.

In addition, the British Universities Finance Directors Group has identified the following areas of potential risk:

- Payments in cash
- Unidentified cash receipts
- Applicants from high risk countries
- Requests for refunds
- Overpayments
- Failure to take up places
- Agents who do not fit in with normal procedures relating to deposits and tuition fees
- Identity fraud.