THE UNIVERSITY of EDINBURGH
Finance

# Anti-Money Laundering (AML) Policy

## Scope and purpose

This policy sets out the University of Edinburgh's (the "University") commitment to understanding and minimising our risks in relation to money laundering and financial sanctions requirements. At the University, we do not condone and have a zero tolerance approach to money laundering, i.e. the process of taking profits from crime and corruption and transforming them into legitimate assets.

This policy applies to all staff of the University of Edinburgh and its subsidiary companies and applies to all expenditure.

## Background

The key elements of the UK anti-money laundering ("AML") framework that apply to universities are listed in Appendix 2. Money laundering is a criminal offence. In the UK, penalties include unlimited fines and/or terms of imprisonment ranging from two to 14 years.

The Money Laundering, Terrorist Financing and Transfer of Funds (information on the Payer) Regulations 2017 (the "MLR2017") replaces the MLR2007 and adopts a more risk-based approach towards AML and due diligence. MLR2017 is more prescriptive, particularly about risk mitigation.

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.

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). Our AML risk report, which must be reviewed at least annually, is attached in Appendix 1.

This statement complements the Criminal Finances Act 2017 statement approved by Central Management Group[1] on 31 October 2017 which sets out the steps the University has taken and will take in relation to preventing the facilitation of tax evasion.

[1] From February 2018, Central Management Group is the University Executive.

# Anti-Money Laundering (AML) Policy

## Our Commitment

The University is committed to tackling malpractice. We will act ethically and with integrity in all our relationships, and use all reasonable endeavours to take action against malpractice, wherever we can do so. The Scottish Code for Higher Education Governance (2017) notes that "the governing body must satisfy itself that the Institution is compliant with all relevant legal and regulatory obligations".

The University has a number of policies and procedures in place to tackle malpractice, including the University's Financial Regulations which are the overarching rules including external regulations which all staff must follow.

In section B of the Financial Regulations, Ethical Principles and Business Conduct, the General Principles state that "no University activity must be undertaken that is in known breach of the laws and regulations of any country. Staff knowingly or recklessly disregarding this prohibition may be subject to disciplinary action, up to and including dismissal. In cases of doubt, all staff must seek advice from the University Secretary before any financial commitment is made or where there is suspicion of money laundering or other criminal activity. All staff must ensure they commit University resources in a transparent and ethical way and must always seek to uphold and enhance the standing of the University."

The Whistleblowing Code of Practice enables staff to report improper conduct or unethical behaviour. The Code of Practice reflects the University's commitment to openness in its affairs and is based on the premise that individuals must feel able to draw attention to perceived malpractice openly and normally within existing procedures and be supported in so doing. Indeed, staff have a duty to report malpractice and are encouraged so to do.

The University also has a number of additional policies which govern our relationships with stakeholders including the Conflict of Interest policy, Anti-Bribery and Corruption policy and Fraud policy.

## Policy

The University has established an appropriate and risk-sensitive policy to minimise our risks in relation to money laundering and compliance with financial sanctions requirements. This policy constitutes the statement of commitment to these six guiding principles and demonstrates the top level commitment required by MLR2017.

### Risk assessment and management

The University has appointed a nominated officer, the Money Laundering Reporting Officer (the "MLRO"), including a deputy, and the contact details can be found in Appendix 4.

The University's statutory risk report is attached in Appendix 1. 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.

# Anti-Money Laundering (AML) Policy

The risk report provides reasonable assurance that the University's AML policies and procedures will support the prevention and detection of money laundering and/or terrorist financing.

## Customer due diligence

As required by the MLR 2017, the University has policies and procedures for performing customer due diligence ("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.

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 explained in Appendix 3. We retain the CDD records relied on for five years from the date on which reliance commences as failure to do so is a criminal offence.

## 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 can use the University's established whistleblowing policy and the Suspected Money Laundering Reporting Form (Appendix 5) to 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 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, 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.

# Anti-Money Laundering (AML) Policy

## 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.

## Compliance management

It is important that our staff and subcontractors understand the compliance culture and the roles and responsibilities placed upon them. Penalties imposed under MLR2017 include fines and imprisonment that can apply to individuals as well as the University.

All staff must understand the University's AML policy and must ask the MLRO if unsure. All staff must report suspicious activity to the MLRO and not discuss what we may or may not report with the customer as 'tipping off' is an offence under the legislation.

## Communication and training

The University's annual Key Commercial Policies compliance ensures that staff are aware of the relevant policies, including money laundering legislation. The AML policy ensures staff understand their responsibilities under the AML regime, the University's due diligence procedures and how to report suspicious activity. The policy is published on the University's Finance website and communicated to staff via internal communication, such as the Finance bulletin.

## Equality and diversity

There are no equality and diversity impacts of this policy.

## Support

Please contact the MLRO or finance.helpline@ed.ac.uk for further information.

Please contact finance.helpline@ed.ac.uk if you require this policy in an alternative format.

## Useful Links

Finance Policies and procedures

# Anti-Money Laundering (AML) Policy

## Approval and review

| | |
|---|---|
| Policy owner | Director of Finance |
| Date policy approved | 20/11/2018 |
| Policy approved by | University Executive |
| Date of commencement of policy | 1st December 2018 |
| Date for review of policy | 1st December 2019 |
| Policy review by | MLRO |
| Policies superseded by this policy | n/a |

## Version control

| Version | Amendment made | Approval date | Approved by |
|---|---|---|---|
| 1.0 | First version | 20/11/2018 | University Executive |
| 1.1 | Update contacts | 11/01/2019 | n/a |

# Anti-Money Laundering (AML) Policy

## Appendix 1 Risk report

The University has undertaken a risk assessment of our current operations. The University's AML controls and processes are deemed proportionate to the financial crime risks and relate to the primary risks identified of jurisdiction, sanctions, customer/third party and operations.

1. Jurisdiction
   1.1. We recognise that there are risks associated with transacting with certain locations and jurisdictions including, but not limited to, the University's countries of operation, the location of customers, suppliers and agents.
   1.2. We also recognise that there are countries that are known to have inadequate AML controls & processes, countries subject to sanctions, embargoes, countries identified as supporting terrorism and/or terrorist organisations. We monitor relevant websites to review sanctioned parties and ensure that the University does not transact with sanctioned parties and regimes.
      - Customer Due Diligence including new customer checks from Creditsafe.
      - The University's Bank Transfer and Online Payment 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.

2. Sanctions
   2.1. The MLRO is responsible and will monitor the relevant websites to review Sanctioned Parties to ensure that the University does not transact with sanctioned parties or regimes.
      - WUBS and the banks provide checks that payments to sanctioned regimes are not made.

3. Customer/third party risks
   3.1. It is not possible to give a definitive list of ways to identify suspected money laundering or how to decide whether to make a report to the MLRO. However, the following indictors are types of risk factors which may, either alone or collectively, suggest the possibility of money laundering activity:
      - A new customer, business partner or sponsor not known to the University. New customer due diligence (CDD) must be performed before transacting with a new customer and our CDD follows the principles of Know Your Customer (KYC) outlined in Appendix 3.
      - A secretive person or business that, for example, refuses to provide requested information without a reasonable explanation. In order to satisfy the requirements, identity checks for money laundering purposes are carried out.
      - A payment of any substantial sum in cash (over £10,000). We do not accept cash as payment for any outstanding debt to the Finance department.
      - Concerns about the honesty, integrity, identity or location of the people involved or absence of any legitimate source for the funds received. In order to satisfy the requirements of KYC, 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). KYC also involves ascertaining and verifying (if appropriate) the identity of the beneficial owners of a business, if there are any, so that we know the identity of the ultimate owners or controllers of the business.
      - Involvement of an unconnected third party without a logical reason or explanation.

# Anti-Money Laundering (AML) Policy

- Overpayments for no apparent reason, especially when refunds are requested. And the cancellation, reversal or requests for refunds of earlier transactions. Refunds are not paid in cash by the University.
  - The Credit balance refund policy for overpayments requires appropriate documentary evidence and/or sponsor payment will be required prior to the refund is authorised.
  - Student refunds are processed via WUBS who carry out compliance checks. Sponsors are encouraged to pay stipends directly to students and not via the University to avoid overpayments of amounts due to the University.
- Significant changes in the size, nature, frequency of transactions with a customer without a reasonable explanation.
- Requests for account details outside the normal course of business.
- A history of poor business record keeping, poor controls or inconsistent dealing.
- Any other facts which tend to suggest that something unusual is happening and give reasonable suspicion about the motives of individuals.

3.2. Where staff know or suspect that money laundering activity is taking place, or has taken place, or are concerned that a transaction may be in breach of regulations, it must be disclosed immediately to the MLRO. The University, through the MLRO, will take all reasonable steps to identify, investigate and, where necessary, report suspicious transactions, of all types.

4. Operations & services

4.1. Student finance

- Student fees & refunds
  - WUBS complete compliance checks for incoming student fee payments to the University from 'designated' individuals, entities or countries/regions.
- Student bank accounts
  - We do not set up student personal bank accounts. The University provides a standard letter for students to set up personal bank accounts.

4.2. Procurement - engaging with contractors or suppliers who are 'designated' or from sanctioned countries/regions.

- The University is committed to contracting only with suppliers and contractors that comply with all appropriate and relevant legislation. The University Procurement Strategy ensures that, where appropriate, and on any given contract, the University will assess the legislation and University policies applicable prior to a procurement and take steps to ensure bidders comply with such legislation. If proportionate, the University may also assess compliance of subcontractors, and request changes if risks are identified in bids or during contracts.

4.3. Research - research activity and collaborations with partners in sanctioned countries/regions or with 'designated' individuals.

- As 4.2 Procurement for payments. New customer due diligence (CDD) must be performed before transacting with a new customer and our CDD follows the principles of Know Your Customer (KYC) outlined in Appendix 3.

4.4. Investment – endowments, donations, bequests and pledges

- New customer due diligence (CDD) must be performed before transacting with a new customer and our CDD follows the principles of Know Your Customer (KYC) outlined in Appendix 3.

4.5. We do not have any known risks associated with PEPs (Politically Exposed Persons).

# Anti-Money Laundering (AML) Policy

4.6. Cash transactions

- We do not accept cash for payment of outstanding debt to the University. We do not accept anonymous payments or payments from unknown third parties although we respect donor requests for anonymity.

5. Risk mitigation
   5.1. The policy is proportionate to the specific risks identified.
   5.2. The AML policy has been approved by senior management.
   5.3. We have both internal controls (with a senior staff member responsible for MLR 2017) and external controls such as the banks who monitor and prevent transactions with sanctioned regimes.
   5.4. We have CDD procedures agreed for transacting with students, customers and third parties.
   5.5. We have reporting procedures, record keeping & monitoring of risk areas.
   5.6. We review and update the AML and risk report annually and report any changes to committee.

# Anti-Money Laundering (AML) Policy

## Appendix 2 Legislation

Anti-Money Laundering laws that regulate financial systems link money laundering (the source of funds) with terrorism financing (the destination of funds). The key elements of the UK anti-money laundering framework that apply to universities include:

1. Proceeds of Crime Act 2002 (as amended)
2. Terrorism Act 2000 (as amended by the Anti-terrorism, Crime and Security Act 2001)
3. The Serious Organised Crime and Police Act 2005
4. Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ("MLR 2017") that includes the requirements of the EU's Fourth Money Laundering Directive (4MLD)
5. Counter-terrorism Act 2008, Schedule 7
6. HM Treasury Sanctions Notices and News Releases
7. Joint Money Laundering Steering Group (JMLSG) Guidance

Offences include:

1. failing to report knowledge and/or suspicion of money laundering
2. failing to have adequate procedures to guard against money laundering
3. knowingly assisting money launderers
4. tipping-off suspected money launderers
5. recklessly making a false or misleading statement in the context of money laundering

# Anti-Money Laundering (AML) Policy

## Appendix 3 Customer Due Diligence (CDD) principles

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.

## Appendix 4 Money Laundering Reporting Officer (MLRO)

The University has appointed the nominated person/money laundering reporting officer (MLRO)

The University's MLRO is the Deputy Director of Finance:

Contact:
Lee.Hamill@ed.ac.uk
0131 650 9552
University of Edinburgh Finance, Charles Stewart House, 9-16 Chambers Street, EH1 1HT

The MLRO is available to discuss any matters relating to the firms policies and procedures relating to the Money Laundering Regulations and helping you understand your obligations.

In the absence of the MLRO the deputy/assistant MLRO has been appointed.

The University's deputy/ assistant MLRO is the Director of Specialist Services:
Contact:
Terence.Fox@ed.ac.uk
0131 650 2166

University of Edinburgh Finance, Charles Stewart House, 9-16 Chambers Street, EH1 1HT

# Anti-Money Laundering (AML) Policy

## Appendix 5 Suspected Money Laundering Reporting Form

| **CONFIDENTIAL - Suspected Money Laundering Reporting Form**<br>*Please complete and send this to the MLRO using the details below* | |
|---|---|
| From: | School/Unit: |
| 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 of Edinburgh: | |
| 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: |
| MLRO contact details:<br>Contact: Deputy Director of Finance<br>Email: Lee.Hamill@ed.ac.uk<br>Address: University of Edinburgh Finance Department, Charles Stewart House, 9-16 Chambers Street, Edinburgh, EH1 1HT<br>Phone number: 0131 650 9552 | |
| *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 five years' imprisonment and/or an unlimited fine.* | |

# Anti-Money Laundering (AML) Policy

## Appendix 6 The University's structure and activities

The University is constituted by the Universities (Scotland) Acts 1858 to 1966. The Universities (Scotland) Acts make specific provision for three major bodies in the Governance of the University: Court, Senate and General Council. The University is organised in three Colleges (College of Arts, Humanities & Social Sciences, College of Medicine & Veterinary Medicine and College of Science & Engineering) and three Support Groups (Corporate Services, Information Services and University Secretary's Group). The University educates students from all over the world and has offices in Edinburgh, Midlothian, Beijing, Mumbai, Santiago, New York and Singapore. It seeks to attract, develop, reward and retain the best staff for a world class teaching and research institution, and develops research, knowledge exchange and teaching partnerships and collaborations across the world.

## Appendix 7 Glossary of Anti-Money Laundering terms and abbreviations

| | |
|---|---|
| **AML** | Anti-Money Laundering is the abbreviation used when referring to relevant legislation and regulation and their enforcement. |
| **Beneficial Owner** | The person(s) who ultimately owns an asset - in Know Your Customer (KYC), this is the key individual(s) about whom checks need to be carried out. On occasions, particularly with offshore entities, the identity of the beneficial owner may not be disclosed in the public domain. Sufficient KYC checks will not be deemed to have been carried out if the identity of the beneficial owner(s) is not established and then subjected to verification. |
| **CDD** | Customer Due Diligence |
| **CFA** | Criminal Finances Act |
| **CFT** | Combating the Financing of Terrorism |
| **Correspondent Bank** | A legitimate banking arrangement where a bank accepts deposits and performs banking services for another bank. There is a specific money laundering risk where the bank using the services is a 'shell bank'. |
| **FATF** | Financial Action Task Force on Money Laundering |
| **Financial Sanctions ('Sanctions')** | Financial sanctions are imposed by the UK and other governments and may apply to individuals, entities and governments, who may be resident |

# Anti-Money Laundering (AML) Policy

| | |
|---|---|
| | in the UK or abroad. Financial sanctions orders prohibit an organisation from carrying out transactions with a person or organisation (known as the 'target'). These measures can vary from the comprehensive - prohibiting the transfer of any funds to a sanctioned country and freezing the assets of a government, the corporate entities and residents of the target country - to targeted asset freezes on individuals/entities. |
| **Integration** | The third and final part of the money laundering process whereby the funds that were originally a direct result of, and directly associated to, criminal activity are fully integrated into the banking system and are thus now clean. |
| **KYC** | Know Your Customer is one of the fundamental precepts of global anti-money laundering regulations. |
| | The process whereby the identity of a new customer must be established before a business or financial relationship can begin or proceed. |
| **Layering** | The second stage of the money laundering process where funds are split up and given more authenticity and a better provenance by financial tools such as shares, stocks, loans and any other mechanism that pushes the criminal money further into the monetary system and thus disguises its origins. |
| **MLRO** | Money Laundering Reporting Officer |
| **NCCT's** | Non-cooperative countries and territories - FATF abbreviation for 'blacklisted' countries and territories. |
| **Offshore Bank** | These are primarily banks that are domiciled in an offshore financial centre and conduct their business with non-residents of that jurisdiction. Sometimes they have no physical presence in the jurisdiction, very little regulation, zero or low tax rates and/or little or no capital reserve requirements. Because of these factors they are an ideal money laundering vehicle but also should be recognised that there are many legitimate offshore banks. |
| **PEP** | Politically Exposed Person. In broad terms, PEP is a term describing someone who has been entrusted with a prominent public function and are usually voted into office. A PEP generally presents a higher risk for |

# Anti-Money Laundering (AML) Policy

| | |
|---|---|
| | potential involvement in bribery and corruption by virtue of their position and the influence that they may hold. |
| **Placement** | The initial and most difficult stage of the money laundering process; this is where the direct results and proceeds of crime are inserted into the business and banking system. There is a vast variety of methods used but the key objective is to make all amounts resemble legitimate business transactions. |
| **SAR** | Suspicious activity report or reporting is a generic term that may have a different title in individual countries. The report(s) submitted by financial institutions and other bodies subject to AML regulations when suspicious money laundering activity is suspected. |
| **Shelf Company** | A pre-formed company which has not normally started trading and can be bought from a third-party provider of company management services. There is also the possibility in some jurisdictions to buy shelf companies that have previously traded but are now dormant or appear to have been legitimately in existence for a number of years because the company was established many years previously. These companies provide the easiest way to start trading but simultaneously create money laundering risks, particularly when the identity of the beneficial owner(s) is hidden. |
| **Smurfing** | A technique used in the placement of funds that are being laundered, where the funds are divided into smaller amounts so that such amounts fall below the threshold at which the financial institution (or other body) is required to file a suspicious transaction report. |
| **Terrorist financing/funding** | The funding of terrorism through a variety of sources and the holding/distribution of these funds to frontline terrorists. Terrorist financing/funding is not money laundering, although the laundering process can be one of the tools used to manage relevant funds. |