

Anti Money Laundering Policy and Procedures

January 2017

Compliance with the Anti Money Laundering Policy (AML) is compulsory. The AML Policy applies to:

- members of the University Board of Governors and other Committees
- staff directly or deemed employed by the University and/or subsidiary or associated companies;
- staff directly or indirectly employed by overseas offices and branches;
- associate lecturers;
- agency staff working for the University;
- any other third parties who work on delivering University services and are paid through a contract for services.

Failure to comply with money laundering regulations can be a criminal offence with up to 14 years imprisonment if convicted. In addition fines and penalties can apply to employees and Board and Committee members.

Members of staff must ensure that they understand the requirements and attend the appropriate training and development sessions offered by the Finance Directorate.

Further guidance and support is available from your named contacts within the Finance Directorate.

Owner:	Chief Finance and Planning Officer
Version number:	2.0
Last revised date:	January 2017
Next revision date:	January 2018

Contents Page

1. Introduction	Page 2
2. What is money laundering	Page 2
3. What are the main offences?	Page 2
4. The Universities policy on anti money laundering (AML)	Page 3
5. University obligations	Page 3
6. Obligations for members of staff	Page 3
7. How is it likely to affect me?	Page 4
8. Persons that the University must not accept as customers	Page 4
9. Knowing your customer (KYC)	Page 4
10. The Money Laundering Reporting Officer (MLRO)	Page 5
11. Disclosure procedure to be followed by staff	Page 5
12. Action and disclosure by the MLRO	Page 6
13. Record keeping procedure	Page 7
14. Acknowledgement of original sources	Page 7
15. Appendix 1 - Suspected money laundering - Report to the MLRO	Page 8
16. Appendix 2 - Guidance note - Possible signs of money laundering	Page 9

1 Introduction

There have been significant political and legislative changes that mean that all organisations have to consider the impact of money laundering on their activities. It is not just a concern for banks and the financial services sector, but also applies to all companies and institutions including Universities.

Therefore the University has implemented a policy and procedures to meet the legislative requirements and to support the mitigation of the risks to the organisation and individuals.

The UK anti-money laundering legislative framework includes:

- Proceeds of Crime Act 2002 (as amended);
- Terrorism Act 2000 (as amended);
- Money Laundering Regulations 2007.

2 What is money laundering?

Money laundering is a crime and is usually described as the process of turning the proceeds of crime into property or money that can be accessed legitimately without arousing suspicion. The term 'laundering' is used because criminals turn 'dirty' money into 'clean' funds which can then be integrated into the legitimate economy as though they have been acquired lawfully.

Universities, like any other organisation, can be targeted as conduits for money laundering, but in practice they may have a greater vulnerability because being associated with a University may give a veneer of public respectability to an enterprise that is in reality dubious or possibly criminal.

Money laundering comprises three distinct stages:

- 1. Placement -** movement of criminal proceeds from their source. For example, cash proceeds from crime may be paid into a bank or used to buy goods, property or assets.
- 2. Layering -** undertaking transactions to conceal the origin of the money. For example, goods or other assets may be resold or funds transferred abroad.
- 3. Integration -** movement of laundered money into the economy so that it looks as if the money came from legitimate sources. For example, invoices from a 'front' company may be paid using cash which originated as the proceeds of crime. Laundered cash can also be loaned to such a company.

3 What are the main offences?

There are 3 principal offences:

Concealing is where someone knows or suspects a case of money laundering but conceals or disguises it.

Arranging is where someone is involved in arranging money laundering.

Acquisition is where someone seeks to benefit from money laundering by acquiring, using or possessing the property concerned.

There are also two 'third party' offences:

- **failure to disclose** one of the three principle offences named above;
- **'tipping off'** – someone informs people who are suspected of being involved in money laundering, so that any investigation of them is likely to be prejudiced.

4 The University's policy on anti money laundering (AML)

The University's policy is to:

- prevent, wherever possible, the University and its members of staff from being exposed to money laundering;
- to identify the potential risk areas where it may occur;
- to comply with all legal requirements, especially reporting actual or suspected cases of money laundering.

The 2007 regulations place emphasis on a risk-based approach to countering money laundering and terrorist financing. The University's policy will ensure that the risks are identified and the likely impact assessed. The detailed procedures will support the mitigation of the risks identified.

5 University obligations

The University has a responsibility to:

- appoint a Money Laundering Reporting Officer (MLRO) to receive, consider and report as appropriate, disclosure of suspicious activity reported by employees;
- implement a procedure to enable the reporting of suspicious activity;
- maintain customer identification procedures to 'know your customer' (in relevant circumstances);
- maintain adequate records of transactions.

6 Obligations for members of staff

Money laundering legislation applies to all members of staff. Potentially any member of staff could be committing an offence under the money laundering legislation 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 [MLRO](#).

Members of staff need to be aware that telling someone you have reported them to the MLRO or the appropriate authorities, or telling them that you are stopping dealing with them or even not giving them an answer where one is expected, could in some circumstances constitute 'tipping off'.

Guidance on how to raise any concerns is included in this policy document. Failure to follow the AML policy may result in you being personally liable to prosecution.

7 How is it likely to affect me?

It is unlikely that a member of staff would commit one of the three principal offences. However, there could be occasions where members of staff have a suspicion of money laundering activities.

For example, a member of staff in the course of their normal duties is collecting payments from international students on behalf of the University. If during the course of taking a payment from a particular student it transpires that the payment is actually being made by an unrelated and or unknown third party and not the student, then the member of staff should raise their suspicions to the Money Laundering Reporting Officer (MLRO). If the member of staff does not report their suspicion and it is later proven to relate to an actual crime, then they would be committing a criminal offence.

The money laundering regulations apply to **cash transactions**¹ in excess of 15,000 Euros (approximately £12,000 at an exchange rate of 1.2 Euro: £1). However the Proceeds of Crime Act applies to **all transactions** and can include dealings with agents, third parties, property or equipment, cheques, cash or bank transfers. In practice at the University customer details are referred to for all face to face transactions and telephone card transactions are processed through our secure system, details are collected as per banking guidelines and the system would alert/decline accordingly.

For other types of transactions checks are made for transactions over £10,000 and for amounts less than this if a higher level of potential risk has been identified.

Another example that a member of staff may encounter is a large and or unexplained overpayment from, or on behalf of, an international student (slight foreign exchange differences are acceptable). Members of staff may receive requests for the element of overpayment to be paid over to a third party - this may constitute money laundering and the money laundering regulations require that the payment is returned to the originating source.

Care should also be taken in respect of refunds requested by a customer. All refunds, where possible, must be made to the original payee using the same payment method as that used by the customer to pay the University.

8 Persons that the University must not accept as customers

The Government may direct businesses not to enter into business relationships or transactions with certain individuals who are subject to financial sanctions. The University must follow the latest guidance in terms of sanctions currently in force in the UK.

A list of all sanctions currently in force in the UK is maintained by HM Treasury. This list can be found at: <http://www.hm-treasury.gov.uk/financialsanctions>

9 Knowing your customer (KYC)

It is important that controls are in place to identify the student, customer or other party dealing with the University. Satisfactory evidence of identify must be obtained. Examples include passport, visa, birth certificate, correspondence with students at their home address. For third parties, letters or documents proving name, address and relationship can be cross referenced with a customer's website or Companies House and the identities of directors can be confirmed. Cheques drawn or payments originating from unusual or unexpected sources should always be verified with regard to the validity of the source.

The requirement to 'know your customer' and the associated due diligence applies for new customers and should be applied on a risk sensitive basis for existing customers. Ongoing customer due diligence must also be carried out during the life of a business relationship, but should be proportionate to the risk of money laundering and terrorist funding. A guidance note on the possible signs of money laundering is included at [Appendix 2](#).

¹ The definition of 'cash transactions' includes payments of physical cash, vouchers or anything equivalent to cash, cheques, debit and credit card payments (including customer not present), direct debits, recurring card payments, online payments and any other payment method not specifically mentioned that results in the University receiving cash into one of its bank accounts.

10 The Money Laundering Reporting Officer (MLRO)

The University has followed best practice and has appointed a MLRO to act as the focal point of all activity relating to money laundering and other criminal conduct.

MLRO - **Simon Taylor** (Assistant Director of Finance)
- Tel: 0114 225 3509
- Email: simon.taylor2@shu.ac.uk

The MLRO's responsibilities include:

- oversight of the organisation's compliance with money laundering and terrorist financing laws and regulations;
- receiving reports from members of staff of their suspicions and deciding whether these should be reported to the National Crime Agency (NCA);
- making external, confidential reports to NCA;
- record keeping of all incidents and actions taken;
- reporting to the Vice-Chancellor and Audit Committee annually.

11 Disclosure procedure to be followed by members of staff

When you either know or suspect that money laundering activity is taking or has taken place, or if you become concerned that your involvement in a transaction may amount to a breach of the 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.

If you have any concerns at all that your line manager is directly or indirectly implicated in the activity you **must not** discuss it with them first and you must contact the MLRO directly and as soon as possible. This is important as a member of staff could commit the 'tipping off' offence even if they were to 'innocently' discuss their concerns with someone whom they believed were implicated.

The disclosure to the MLRO should be made on the proforma reported attached at [Appendix 1](#) and should be completed as soon as possible following the confirmation of reasonable suspicion. **Should a member of staff not follow this process they could be personally liable to prosecution under the regulations.**

Your report should include as much detail as possible including:

- Full details of the people, companies involved including yourself and other members of staff if relevant;
- full details of the transaction(s) 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 information that may help the MLRO consider the case for knowledge or suspicion of money laundering and to facilitate the report to the Serious Organised Crime Agency (NCA).

Once you have reported your suspicions to the MLRO you must follow any instructions provided. You must not make any further enquiries unless instructed to do so by the MLRO. At no time and under no circumstances should you voice any suspicions to the person(s) you suspect of money laundering.

If appropriate the MLRO will refer the case to the NCA who will undertake any necessary investigation. This may include consent to continue with a particular transaction and care should be taken not to 'tip off' the individuals concerned, otherwise you may be committing a criminal offence.

12 Action and disclosure by the MLRO

On receipt of a disclosure report the MLRO will:

- note the date of receipt and acknowledge receipt of it;
- assess and advise the individuals concerned when a response can be expected;
- consider the report and any other relevant information, undertaking further enquiries necessary to decide if a report should be made to the NCA.

Once the MLRO has evaluated the case a timely determination will be made as to whether:

- there is actual or suspected money laundering taking place;
- there are reasonable grounds to know or suspect that is the case;
- consent if required from NCA for a particular transaction to proceed.

Where the MLRO concludes that the case should be disclosed to NCA this needs to be done:

- in a timely manner;
- in the manner prescribed at <http://www.nationalcrimeagency.gov.uk/contact-us/reporting-suspicious-activity-sar>

Where the MLRO concludes that there are no reasonable grounds to suspect money laundering then consent will be given for transactions to proceed and the disclosure report will be marked accordingly.

13 Record keeping procedure

All disclosure reports and relevant documents will be retained in a confidential file by the Finance Directorate for a minimum of six years.

Other documentation that may be required under this legislation should be retained in accordance with the University's [records management intranet page](#).

14 Acknowledgement of original sources

This AML policy and associated procedures have been prepared by the Finance Directorate. This document contains content reproduced extensively from third party sources and it is acknowledged that the following organisations materials have been reproduced:

- University of Bradford - Anti-Money Laundering Policy
- London Metropolitan University - Anti-Money Laundering Policy
- Suffolk County Council - Anti Money Laundering Guidance Notes
- British Universities Finance Directors Group (BUDFG) - notes on money laundering prepared by Grant Thornton UK LLP 2007

Appendix 1 Suspected Money Laundering - Report to the MLRO

From:..... Faculty/Directorate.....

Contact Details.....

DETAILS OF SUSPECTED OFFENCE

Name(s) and address(es) of person(s) involved including relationship with the University:

Nature, value and timing of activity involved:

Nature of suspicions regarding such activity:

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 2 Guidance Note - Possible signs of money laundering

It is impossible to give a definitive list of ways in which to spot money laundering or how to decide whether to make a report to the MLRO (Money Laundering Reporting Officer). However, the following are types of risk factors which may, either alone or cumulatively with other factors, suggest the possibility of money laundering activity:

- A new customer, business partner or sponsor not known to the University;
- A secretive person or business e.g. that refuses to provide requested information without a reasonable explanation;
- Payment of a substantial sum in cash (over £10,000);
- Concerns about the honesty, integrity, identity or location of a client;
- Illogical third party transactions: unnecessary routing or receipt of funds from third parties or through third party accounts;
- Involvement of an unconnected third party without logical reason or explanation;
- Overpayments by a customer for no apparent reason;
- Absence of any legitimate source of the funds;
- Movement of funds overseas, particularly to a higher risk country or tax haven;
- Where, without reasonable explanation, the size, nature and frequency of transactions or instructions (or the size, location or type of a customer) is out of line with normal expectations;
- A transaction without obvious legitimate purpose or which appears uneconomic, inefficient or irrational;
- The cancellation or reversal of an earlier transaction;
- Requests for the release of customer account details other than in the normal course of business;
- Companies and trusts: extensive use of corporate structures and trusts in circumstances where the customer's needs are inconsistent with the use of such structures;
- A history of poor business records, controls or internal accounting controls;
- A previous transaction for the same client which has been, or should have been, reported to the MLRO.