Anti-Money Laundering Policy

Contents

1. Policy Aim

On 26th June 2017 the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 came into force, in place of the Money Laundering Regulations 2007 and applies to all companies including Universities.

The Finance Division is responsible for ensuring that a written University-wide Anti Money Laundering Policy is in place to prevent and detect money-laundering activity. The policy will ensure that reasonable and proportionate controls are put in place, risk assessment and due diligence is undertaken and regularly reviewed to ensure that the requirements of the regulations and legal obligations may be properly met. This policy applies to all University of Leicester staff.

2. Money Laundering

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. Money laundering regulations apply to cash transactions in excess of 10,000 euros. However, the Proceeds of Crime Act applies to all transactions – cheques, cash, bank transfers, property and equipment to individuals or agents or third parties.

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

a) **Placement** is where the proceeds of criminal activity enter into the financial system;
b) **Layering** is moving the money from its illegal source through layers of financial transactions;
c) **Integration** involves the re-introduction of the illegal proceeds into legitimate commerce by providing an apparently genuine explanation for the funds.

Most anti-money laundering laws that regulate financial systems link money laundering (which is concerned with source of funds) with terrorism financing (which is concerned with destination of funds).

In the UK, severe penalties are imposed on individuals connected with any stage of laundering money, including unlimited fines and/or terms of imprisonment. Offences include:

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

Key elements of the UK AML framework that apply to universities include:

- 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

Failure to report a suspicious payment is a criminal offence, which may result in prosecution of an individual.

Further information on Money Laundering is found on the UK Government website; https://www.gov.uk/government/publications/anti-money-laundering-guidance-for-money-service-businesses

3. Risk-Based Approach

There is no exact definition and criteria as to what constitutes suspicion defined in legislation and the University will take all reasonable steps to identify suspicious transactions and will consider all relevant available information. If any doubt remains after considering the information available, the suspicious payment is to be reported. The University of Leicester will adopt a risk-based approach to prevent and detect money laundering:

- Appoint a University Nominated Officer and a Deputy Nominated Officer
- Provide staff awareness and training
- Ensure appropriate due diligence checks are undertaken
- Apply 'know your customer' principles
- Not accept cash payments in person or paid directly into the bank account

- Identifying suspicious activity
- Ensure procedures are in place for reporting and recording of suspicious activity
- Undertake a review of risk assessment approach

4. University Nominated Officer

The Nominated Officer is appointed to act on behalf of the Director of Finance. The University Nominated Officer who is responsible for reporting any suspicious activity that might be linked to money laundering or terrorist financing, will be an employee of the University, the Treasury Accountant. The University has appointed a Deputy Nominated Officer who is the Deputy Director of Finance responsible for Operations and Controls. This person is to be contacted in the absence of the Nominated Officer.

The Nominated Officer is:

- trusted with the responsibility
- senior enough to have access to all your customer files and records
- able to decide independently whether or not they need to report suspicious activities or transactions - a decision that could affect your customer relations

The University Nominated Officer's role is to be aware of any suspicious activity that might be linked to money laundering or terrorist financing, and if necessary to report it. The Nominated Officer is responsible for:

- receiving reports of suspicious activity from employees
- 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 the NCA for a defense to a money laundering offence in relation to the transactions that they've reported, and making sure that no transactions are continued illegally
- ensuring operating anti money laundering controls and procedures are in place
- ensuring money laundering risk assessments are in place ensuring accurate and up to date record keeping
- ensuring staff are trained in preventing money laundering
- employees know who the nominated officer is, what they're there for and how to contact the person
- employees know who the deputy nominated officer is, when to be contacted and how to contact the person
- provides clear guidance and training on spotting suspicious activity and reporting it to the nominated officer or their deputy
- employees are made aware of the anti-money laundering policies, controls, procedures and risk assessments and adhere to them
- making sure employees know where to go for more help or information about the Money Laundering Regulations

5. University Staff Awareness and Training

All University staff are to be made aware of the University policy on money laundering and in particular staff directly involved in financial transactions are provided with clear guidance and training on identifying suspicious activity, their obligations to remain vigilant and how to report concerns to the Nominated Officer.

Completion of a mandatory online training course on fraud, bribery and corruption and the Criminal Finances Act is required by all members of staff annually. A test at the end of the online training course is to be completed, achieving a pass mark of 80%. A record of the date staff members complete and pass is recorded.

6. Due Diligence

The University must be reasonably satisfied as to the identity of the customer (and others) that they are engaging with in a business relationship. The University will take all reasonable steps to identify and report suspicious transactions, of all types. This includes matches involving Politically Exposed Persons (PEP's) and Sanctioned Parties. The University adopts risk-based systems and controls with the aim of mitigating the risk of financial crime.

The four major risks are:

- **Product/Service** Risks associated with the University's standard product and service offerings.
- **Jurisdictional** Risks associated with geography, location and jurisdiction including, but not limited to, the University's countries of operation, the location of customers, suppliers and/or agents, and transactional sources/destinations.
- **Customer/Third-Party** Risks associated with the people and/or organisations that the University undertakes business (in all forms) with including customers/third-parties, beneficial owners, agents, contractors, vendors and suppliers. Politically Exposed Persons (PEP's) and Sanctioned Parties are also considered within this risk.
- **Distribution** Risks associated with how the University undertakes business, including direct and indirect relationships (e.g. via an agent or third-party), face-to-face, digital/online and telephonic.

7. Know Your Customer

For student income, the University collects detailed records of personal information of a student prior to joining the University during the admissions process and the information is maintained during their enrolment with the University, on the University Academic Database SITS.

For Students who are not self-funded and payment is received by an official sponsor, a Financial Guarantee Letter is received from the sponsor on official company headed paper or a Sponsorship Agreement form is received. If applicable checks on the validity of the company will be undertaken. Information about the sponsor is recorded on the University Academic Database SITS.

When payments are made using the online payment portal for student tuition or accommodation, the student number and date of birth is required and also the payee relationship.

For payments via the online store, an invoice number is required.

For bank transfers paid directly into the University bank account, payees are advised to quote the student number or invoice number as a payment reference.

The University also maintains a list of sanctioned countries from which payments are not accepted in line with banking regulations. The University carries out regular checks on payments received for students whose country of domicile is also on the sanctioned country list. Students are required to provide evidence of payment source in order to comply with regulations.

The University has an obligation to conduct its fundraising operations and relationships in an ethical manner and to ensure that due diligence is undertaken when assessing whether to accept philanthropic gifts or establish specific philanthropic relationships. The University has a separate Gift Acceptance: Due Diligence Policy, which includes the checks undertaken for this source of income.

For non-student income, departments of the University that collect income such as Research Finance, Attenborough Arts, Estates and Campus Services, Sports Centre, Departments undertaking business with external customers ensure that due diligence is observed when assessing whether to accept income.

Having completed due diligence on income received, the University will assess, as outlined above, the money laundering and terrorist finance risk associated with the transaction received.

8. Reporting and Recording Suspicious Income

Any individual who has suspicions or concerns of actual or suspected activities must report in writing to the Nominated Officer or in their absence to the Deputy Nominated Officer immediately. Once reported, staff should make no further enquiries into the situation or discuss the matter with anyone else unless instructed by the Nominated Officer to avoid hindering any investigation. Failure to report a suspicious payment is a criminal offence, which may result in prosecution of an individual.

The Nominated Officer, will review the information, carry out any additional investigation and if deemed necessary on any suspicious activity or transaction, submit a Suspicious Activity Report (SAR) to the National Crime Agency (NCA). Action Fraud, Director of Finance and the Audit and Assurance Committee are to be informed, as well as referral to the Admissions Team or Student and Academic Services.

The University will maintain adequate records of suspicious income, which are appropriate to the scale, nature and complexity of the income. These records include when applicable; identity information, identify documents, transaction information, transaction records, evidence of investigation, records of reports (internal and external). Clear, concise, detailed records of the factors that indicate why it is suspicious, information sought and outcome are to be recorded.

The Nominated Office will keep a separate record of all cases reported to the National Crime Agency along with the Suspicious Activity Reports (SAR's) submitted.

9. Review of Risk Assessment

The Nominated Officer is responsible for ensuring that an annual review of the University policy and procedures is undertaken or if there is a major change in legislation/policy/circumstances. The review will take into account the various risks and vulnerabilities with the university activities and business and those of its customers.

The review will cover:

- review policies and procedures
- review training logs to ensure that all relevant employees have been trained
- where suspicious activity has been flagged, ensure it has been reported in line with the policy
- recording, monitoring and retention of records to ensure they are in compliance with the policy
- identifying any changes in guidance, legislation or regulators. Consider and communicate the impact of any upcoming changes
- record of the review undertaken, highlighting any discrepancies, current or upcoming risks, including and ensuring any changes are implemented.
- if the review highlights any areas of high risk and concern that cannot be addressed by the Nominated Office, these must be reported to Director of Finance as soon as possible.

10. Policy on Payment to Third Parties

The University recommends that students/customers do not transfer funds to third parties to make payment on their behalf as the student/customer cannot be sure that the third party will make legitimate payments to the University. If for any reason the student/customer decides to make payment to a third party, that student/customer may directly or indirectly be complicit in money laundering activity. In addition if the third party fails to pay the University, the student/customer is still liable to remit the required amount to the University.

No payments should be made to an agent or partner of the University with fees paid directly to the University unless otherwise stated in the legal contract. An agent's contract with the University also states that applicants/students should make all payments directly to the University and that agents are not to accept any payments from applicants/students.

11. University Policy on Payment of Refunds

If a refund is requested, repayments will only be made to the person or organisation that made the latest payment and by the same method of payment as the latest payment.

If monies were received from a UK bank account then it will returned using the account details on the remittance received from the University bankers.

If the bank transfer was from outside of the UK then proof of the funds leaving the senders bank account in the form of a statement from that bank, clearly showing the payment made and bank account details is required. This is to ensure that the money is returned to the original payer. If a third party has been used, such as Convera , proof of their payment to that third party is required.

The other exception is where payment has been made by cheque from a UK bank account where the refund will be issued by bank transfer to the same bank account as those on the cheque. Proof of the funds leaving the senders bank account in the form of a statement from that bank, clearly showing the payment made and bank account details is required. This is to ensure that the money is returned to the original payer.

12. Returning Payments

If payment has been made to the University in error, confirmation as to why it was sent, why it should be returned, name of recipient and bank account details it should be returned to (ensure these match the bank account is originated from) is required in writing.

If significant overpayment on an invoice or unexpected amount is received, the person who remitted the money is to provide justifiable reasons as to why an overpayment was made.