Anti-Money Laundering Policy and Procedures

October 2023

Compliance with the Anti-Money Laundering (AML) Policy 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.

Being involved in money laundering, or failing to report a suspicion of money laundering, are criminal offences with penalties of up to 14 years imprisonment if convicted. In addition, fines and penalties can apply to staff and Board and Committee members.

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

Further guidance and support is available from Finance.

Owner:	Chief Finance Officer
Version number:	4.1
Last revised date:	October 2023
Next revision date:	December 2024

Contents

1. Introduction

Sheffield Hallam University **(the "University")** is committed to ensuring the highest standards of probity in all of its financial dealings. It will therefore ensure that it has in place proper, robust financial controls so that it can protect its funds and ensure continuing public trust and confidence in it. Some of those controls are intended to ensure that the University complies in full with its obligations not to engage or otherwise be implicated in money laundering or terrorist financing. This policy sets out those obligations, the University's response and the procedures to be followed to ensure compliance.

The University has a zero-tolerance approach to money laundering and is committed to the highest standards of ethical conduct and integrity in its activities in the UK and overseas.

2. Implementation

The University's Audit and Risk Committee has responsibility for overseeing the University's policies on fraud and irregularity and for reviewing their implementation and effectiveness.

The Chief Finance Officer has day to day operational responsibility for the policy and its implementation.

The University has also identified a Money Laundering Nominated Officer (MLNO) and deputy who are the focal point of all money laundering compliance activity including for receiving suspicious activity reports. Further details of the MLNO's role are set out in Section 11.

The implementation of this policy includes:

- regular assessments of the University's money laundering risks;
- having appropriate due diligence procedures in place, and ensuring these are followed so that risks relating to individual transactions can be identified, assessed, mitigated and kept under review;
- having procedures for reporting any suspicions of money laundering and the actions the University will take where a report is made;
- ensuring money laundering training is delivered within the University including training on this policy; and
- reviewing and, if necessary, updating this policy at least annually (and where needed to respond to new or emerging risks) and monitoring compliance.

Any failures to adhere to this policy may be dealt with under the University's disciplinary or poor performance policies, as appropriate.

Any such failures also expose the individual concerned to the risk of committing a money laundering offence.

3. Introduction to Money Laundering

Money laundering is the process of taking profits from crime and corruption (the proceeds of crime) and dealing with them in such a way as to disguise their criminal origins. The term 'laundering' is used because criminals turn 'dirty' money into 'clean' funds which can then be integrated into the economy as though they have been acquired lawfully.

Money laundering schemes come with varying levels of sophistication from the very simple to the highly complex. Straight forward schemes can involve cash transfers or large cash payments whilst the more complex schemes are likely to involve the movements of money across borders and through multiple bank accounts.

Money laundering is not confined to money or cash in the traditional sense but covers any criminal property i.e. property which is derived from (or is the proceeds of) criminal conduct. It includes all types of money or cash[1], as well as goods or other assets with a value and any profits or gains from the original offence.

Universities, like any other organisation, can be targeted as conduits for money laundering. But there may be particular risks for the sector, for example, the risks associated with financial transactions involving students or partners in overseas (higher risk) territories.

Money laundering schemes typically involve three distinct stages:

1. Placement - movement of criminal property 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 criminal property. For example, goods or other assets may be resold or funds transferred abroad. This distances the criminal property from its illegal source.

3. Integration - movement of criminal property into the legitimate economy so that it looks as if this came from lawful sources.

4. Legislative and regulatory framework

Legislation

In the UK, severe penalties are imposed on individuals connected with any stage of laundering money. Penalties include unlimited fines and/or terms of imprisonment ranging from 2 to 14 years.

There are three main money laundering offences (which are offences under the **Proceeds of Crime Act 2002 (or "POCA"))** these are:

- **the "concealing" offence**: concealing, disguising or transferring the proceeds of crime or removing them from the UK;
- **the "arranging" offence**: entering into or being involved in an arrangement if the person knows or suspects this involves the proceeds of crime; and
- **the "acquisition, use and possession" offence**: acquiring using or possessing the proceeds of crime.

All three offences require either "knowledge or suspicion" of criminal conduct. A suspicion does not have to be clear or firmly grounded, or supported by evidence, provided it is a possibility which is more than fanciful – this is a very low bar to cross.

It is also an offence to fail to report knowledge or suspicion of money laundering.

An offence can also be committed by prejudicing an investigation into money laundering.

There is no minimum financial threshold for money laundering offences, they can apply to money laundering involving any amount. There are also no limitation periods within which a prosecution must be brought.

[1] '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 payment platforms and any other payment method not specifically mentioned that results in the University receiving cash into one of its bank accounts.

UK money laundering offences can be committed even where the proceeds of crime relate to criminal conduct which occurred abroad.

Other relevant obligations

- **Charity law and the Charity Commission**: As an exempt charity, the University's principal regulator is the OfS rather than the Charity Commission. However, the University must still comply with charity law and much of the guidance published by the Charity Commission. The Commission's guidance for charity trustees and its more detailed guidance on due diligence and using charitable funds[2] and fraud and financial crime[3] emphasise trustees' legal duties to protect charitable assets and do so with care including carrying out proper due diligence on payments received by the charity. This in turn require trustees to ensure that proper AML policies controls and procedures are in place.

- **Reporting to the OfS under their regulatory framework**: The University's Money Laundering Nominated Officer (MLNO) must have regard to the OfS guidance on reporting of "reportable events" to establish whether to report suspected or actual money laundering events them[4].

5. Associated Policies

This policy forms part of the University's suite of policies relating to financial crime risks as shown below. All policies are available on the University staff intranet and the University website:

- Anti-bribery policy
- Anti-corruption policy
- Fraud and corruption response plan
- Criminal Finances Act 2017 statement
- Speak Out (Whistleblowing) Policy

6. The University's approach to anti-money laundering (AML)

The University adopts a risk-based approach towards AML and conducting due diligence and reviews the level of risk on an annual basis (see Section 7). Whilst many of the University's financial transactions could be considered relatively low risk from the perspective of money laundering, all staff need to be vigilant against any financial crime and fraud risks that the University may face.

Money laundering could arise in any of the University's transactions including those with students, agents, contractors, suppliers, business or research partners, donors or other third parties, and could involve property or equipment, cheques, card, cash, bank or other financial transactions.

The University's approach to mitigating money laundering risk is based on the adoption of the following five key principles and having procedures in place to meet each of them:

- Obtaining satisfactory evidence of the identity of the customer or third party with whom the University deals and/or has a business relationship (through Know your Customer (KYC) and Customer Due Diligence (CDD) checks – see Section 8). The extent of due diligence required in any case will be guided by the anti-money laundering (AML) risk assessment. The higher the risk associated with the transaction the greater the due diligence which will be required.

- Retaining evidence of the customer / third party's identity, and transactions made with them, for the duration of the relationship and for a period of six years after it terminates.

---

[2] Chapter 2 of the Charity Commission's Compliance Toolkit: Due diligence, monitoring and verifying the end use of charitable funds.
[3] Chapter 3 of the Charity Commission's Compliance Toolkit: Fraud and financial crime.
[4] Under the OfS regulatory framework a 'reportable event' includes: any material suspected or actual fraud or financial irregularity where 'material' should be understood to mean: (i)• any fraud relating to the misuse of public funds; (ii) any other financial fraud exceeding £50,000 in value or 1 per cent of a provider's annual income if that income is less than £5,000,000; or (iii)• any type of non-financial fraud or attempted fraud regarding which the provider determines to notify its own governing body.

- Appointing a Money Laundering Nominated Officer (MLNO) and deputy and establishing a process for reporting any suspicious transaction to the MLNO. Further details of the University's MLNO are included at Section 11.

- Where necessary, the MLNO reporting any suspicion of money laundering to the appropriate authorities. In the UK this is the National Crime Agency (NCA).

- Providing appropriate training to all relevant members of staff who handle, or are responsible for handling, any transactions with the University's clients and/or other third parties – see Section 9. This is to ensure staff are aware of the University's procedures which guard against money laundering and the legal requirements relating to this. The University will keep records of all training undertaken.

7. The University's annual anti-money laundering (AML) risk assessment

The University undertakes an annual money laundering risk assessment in relation to its activities, the current risk assessment is set out at Appendix 1. The University's AML controls and processes are designed to be proportionate and aligned to this assessment. The overall or composite assessment of risk is based on the component risks in the following key areas:

- **Product/Service/Sector risk:** Risks associated with our standard product and service offerings and the sector we work in.

- **Jurisdictional risk:** 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. The risks are higher for countries recognised to have inadequate AML controls and processes, countries subject to sanctions, embargoes and related measures and countries identified by recognised authorities as supporting terrorism and/or terrorist organisations.

- **Customer/Third-Party risks:** Risks associated with the people and/or organisations that we undertake all forms of business with, including customers/third-parties, beneficial owners, agents, contractors, vendors, suppliers, research partners or donors. Cash businesses, unusual business relationships, non-UK establishments, Politically Exposed Persons[5] (PEP's) and sanctioned parties present greater risks.

- **Transaction risk:** Risks associated with how we undertake business, including direct and indirect relationships (e.g. via an agent, intermediary or third-party), face-to-face, digital/online and by telephone. Cash transactions, anonymous transactions, non-face-to-face transactions, transactions involving unknown third parties, unusual transactions and unregulated transactions (i.e. from unregulated third parties) all pose greater risks

New and emerging risks will also be considered including those identified by the National Crime Agency and other relevant sources. This includes, for example, those arising from changes in the way that business is conducted as experienced in the context of Covid-19, the vulnerabilities created by international conflict and instability, the cost of living crisis and poverty, the increased use of technology both in how fraudsters target individuals through social media and online and how they hide their activities.

[5] A politically exposed person (PEP) is someone who's been appointed by a community institution, an international body or a state, including the UK, to a high-profile position within the last 12 months. They present a higher risk because of the political influence which they hold.

8. Due diligence and assessing and managing risk at a transactional level

The University's AML processes and controls for any transaction are designed to reflect our risk based approach and to be proportionate to the potential money laundering risks involved in the context of:

- the customer / third party – knowing your customer (KYC) and customer due diligence (CDD)
- the transaction;
- and the geographical location / jurisdiction.

We will adopt more rigorous checks and controls for higher risk parties or transactions.

Undertaking KYC and CDD ensures that the University complies with the law and mitigates the risks associated with money laundering. It also protects against other financial crime risks and offences under related legislation including: bribery and corruption, counter-terrorist financing, sanctions and export control. It ensures the University acts in accordance with UK Government guidance including guidance from HM Treasury and with our duties as a charity and the Charity Commission's guidance (as referred to in section 4). CDD also makes good business sense by identifying, at an early stage, those relationships which the University should avoid owing to the unacceptable level of risk.

There are a number of components that make up the University's CDD checks, these components are:

- **Ascertaining and verifying the identity of the customer/student/third party** the University should be reasonably satisfied of the identity of the customer, or other third party with whom we intend to engage in a business relationship, i.e. knowing who they are, confirming their identity is valid and verifying this by obtaining documents or other information from sources which are independent and reliable.

- **Ascertaining and verifying (if appropriate) the identity of the beneficial owners of a business and property held in the UK**, so that we know the business's ultimate owners, or controllers of the business.

- **Information on the purpose and intended nature of the business relationship** i.e. knowing what we are going to do with/for them and why.

Our requirement for KYC and the associated CDD apply for new customers/other parties and should be applied on a risk sensitive basis for existing relationships. Ongoing CDD must also be carried out during the life of a business relationship but should be proportionate to the risk of money laundering and other financial crime risk and/or as part of the University's wider relationship management processes.

The University will ensure the CDD records relied on are retained for six years from the date on which reliance commences.

Managing transactional risk

As there are no financial thresholds for money laundering, cash payments are a particular risk. To address this risk, the University does not accept cash payments for tuition fees and its bank (HSBC) will not accept cash payments unless accompanied by a pre-printed paying in slip for the account into which the monies are to be paid..

Where appropriate, we will ascertain the source of funds for a transaction, confirming the funds are legitimate and available.

Managing jurisdictional risk / sanctions

There are a number of sources which identify countries or persons considered to be a high-risk for AML purposes. These sources include those shown in the table at Appendix 2, together with the high risk-jurisdictions and parties which they identify.

If any transaction involves persons/organisations in these jurisdictions, then enhanced due diligence and additional risk assessment is required. The University therefore checks the location of parties it does business with, so it identifies any involvement in these areas and can act accordingly.

The UK's sanctions in force list identifies those persons or entities which the Government directs parties not to do business with. As part of our CDD process, this list should be checked and **Government guidance followed where high risk jurisdictions are involved**.

9. Training and staff awareness

The University will ensure that new members of the Finance Directorate receive appropriate anti-money laundering training as part of their induction process. Refresher training will take place at least every two years, or when the policy is revised.

The policy will be drawn to the attention of other University staff in their induction process. Teams identified as potentially exposed to higher risk (i.e. Alumni & Development, GDP, Overseas offices, BESE (contracts), ULT, Research Institutes, Research and Innovation Services, International Experience, Legal Services) will be asked to complete the on-line anti-money laundering training as part of their induction process and at least every two years.

10. Responsibilities of staff / associated parties under this policy

Potentially any member of staff could be committing a money laundering offence if they suspect money laundering or if they become involved in some way and do nothing about it. All staff must 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.

Guidance and examples on possible signs and red flags for potential money laundering are included at Appendix 3.

If an individual has any suspicion that money laundering has or may be about to take place or that any action they take might involve them in money laundering, the individual must report this as soon as possible to the University's MLNO (see Appendices 4 and 5) and should take no further steps regarding the transaction.

The individual must then co-operate fully with any investigation into the reported concerns. They must:

- maintain confidentiality about any suspected or actual incidents involving the University; and
- make no further enquiries into the situation or discuss their concerns with anyone else at any time, unless instructed to do so by the MLNO. This is to avoid committing an offence by prejudicing the investigation.

The guidance on how to raise any concerns is included at Appendices 4 and 5 of this Policy. Failure to follow the AML Policy may result in the individual being personally liable to prosecution. The University may also follow disciplinary procedures against any member of staff who fails to follow this policy and/or who has committed a money laundering offence. Such disciplinary action could result in dismissal.

11. The Money Laundering Nominated Officer (MLNO)

The University has followed best practice and has appointed a MLNO to act as the focal point of all activity relating to money laundering and other financial crime risks. Details of the appointed MLNO and their deputy are shown below:

MLNO - **Ryan Keyworth** (Chief Finance Officer)

- Tel: 0114 225 5498
- Email: r.keyworth@shu.ac.uk

Deputy MLNO **- Louise Walsh** (Head of Financial Reporting and Compliance)

- Tel: 0114 225 4550
- Email: l.walsh@shu.a.c.uk

The MLNO's responsibilities include:

- oversight of the University'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 as SARs to the National Crime Agency (NCA);
- making external, confidential reports to the NCA;
- record keeping of all incidents and actions taken associated with this policy and the University's procedures for addressing money laundering risk; and
- reporting to the University's Vice-Chancellor and the Audit and Risk Committee annually.

12. Record keeping procedure

The MLNO will keep a Register of Money Laundering Report Forms and will update this register with any relevant documentation.

All disclosure reports, relevant documents and details of investigations will be treated as strictly confidential with access restricted to a limited number of individuals i.e. only those who require access on a need to know basis (including the MNLO and their deputy, Head of Financial Reporting and Compliance, Legal Services and key support staff). Records will be retained for a minimum of six years.

Other documentation that may be required should be retained in accordance with the University's Records Management SharePoint page.

Appendix 1 Anti-money Laundering Risk Assessment – October 2023

Overall Risk Rating: LOW

The risks of money laundering for the University and for the UK HEI / not-for-profit sector as a whole are generally considered to be low[6]. However, as shown by the table below there remain areas of vulnerability or increased risk which the University seeks to manage and address through the accompanying mitigations or controls. No single risk factor should be viewed in isolation as the level of risk will usually depend on the presence (or not) of other risk factors. The National Crime Agency has also recently reported[7] that the threat from money laundering in the UK is increasing.

The particular and current sector risks were initially highlighted in a report in the Times in February 2021 which identified at least 49 British Universities accused of the inadvertent money laundering of approximately £52 million through the acceptance of cash payments for tuition fees from students in high risk countries including China, India, Russia and Nigeria. More recent media reports[8] continue to highlight the risk to universities through taking cash payments. As such, this risk remains as at October 2023.

There also continues to be increasing evidence of fraudsters targeting and recruiting students (often through social media) to act as "money mules" and a report[9] that in the first six months of 2023, one in five of UK money mule cases involved people under 21. New students having their first taste of independence can be particularly vulnerable to this, particularly in the current cost of living crisis, which brings an added responsibility for the University to make our student community aware of these risks and how to guard against them (and particularly for our international students).

An example of the component money laundering risk associated with payment of tuition fees could be illustrated with the RAG rating table shown below:

Risk Rating		Nationality / Domicile	Person making the payment and their relationship with the student	Payment method
	Low	UK	Student	UK card payment / UK bank transfer
2	Low	EU	Parent/Guardian	International card
3	Medium	Non-UK or EU	Other relative	Third party provider / multiple payments
4	High	Non-UK or EU	Unrelated	International bank transfer
5	High	High risk jurisdictions	Unknown/suspicious and/or multiple payers	Cash or suspicious payment patterns

[6] HMT and Home Office joint National Risk Assessment of Money Laundering and Terrorist Financing 2020 (published December 2020)
[7] NCA – National Strategic Assessment 2023.

Risk type	Description of Risk	Risk mitigation/control	Risk assessment
Product / service	**Payment of Tuition Fees:** The University allows the payment of student fees via a variety of arrangements (e.g. student loan company, sponsors, self-financing). As illustrated in the table above, the money laundering risks arise from payment arrangements where the payment is received from unknown and/or unverified third parties with little or no relationship to the student and/or through the type of payment method used. Payments for students from a high-risk jurisdiction are similarly higher risk.	Most risks are mitigated by the funds being paid direct to the University i) by the student, whose identity will have been verified, or ii) the student loan company, that is a recognised and valid source of funds. Third party payments are only accepted where the third party has been authorised by the student and is closely related to them, or where a sponsor has been verified. Students are encouraged to make the payment through recognised and validated payment methods identified as such on the University's website. The University is now able to take payments from international students through the Flywire platform, which allows them to make payments via international credit cards or via bank transfer. All payments are made to Flywire and then Flywire makes the payment to the University. Flywire is FCA regulated and so has sophisticated inbuilt checks using artificial intelligence and machine learning to try and identify and therefore stop potentially fraudulent transactions. Our overseas offices and international experience team raise student awareness and encourage them to be vigilant for attempts to draw them in to money mule activity.	**Low**
	Donations: The University receives "donations" to further its charitable objectives. The money laundering risks arise from donations where the funds come from unknown and/or unverified third parties.	The University has a Donation Acceptance Policy, which provides guidance for staff on the acceptance of philanthropic donations ('gifts'). Staff must advise the Development and Alumni relations Office of any donations that they are soliciting or negotiating to support the University. A Due Diligence Oversight Group will advise on the appropriateness of all potential donations over £5,000. Donations less than	**Low**

[8] Guardian 7 September 2023 – UK Universities still taking cash payment for fees 'is money laundering risk'
[9] Financial Times 12 July 2023 – Under 21s targeted by money launderers, warns UK fraud agency

Risk type	Description of Risk	Risk mitigation/control	Risk assessment
		£5,000 will be reviewed by the Head of Development and Alumni Relations. Further reviews will be carried out at Group Director level for donations up to £50,000 and for donations above that and up to £1m will be considered by the VC / Deputy VC and CFO. Any donations over £1m will be considered by UEB and may require sign off by the Board of Governors. The University will not accept donations of crypto currency, due to difficulties in verifying ownership. This is particularly important as crypto currency is a known facilitator through which fraudsters launder the proceeds of crime.	
	Payments for services and funding: The University receives payments for services, grant funding and private sector funding or contributions through a variety of sources both in the UK and overseas.	We apply customer and partner due diligence processes to proposed business relationships.	**Low**
Jurisdiction	The University operates in both the UK and overseas territories, with some of its activities being undertaken in potentially higher risk locations.	All activities with overseas partners are subject to rigorous due diligence procedures. Following the introduction of the Economic Crime (Enforcement and Transparency) Act 2022 there are various measures being introduced to increase the transparency and accuracy of information on companies (i.e. beneficial owners) held by Companies House, including a new register of overseas entities that own land or property in the UK. These measures will be further enhanced when the Economic Crime and Corporate Transparency Bill is enacted. The University will use this information in its due diligence process, where appropriate. The University has had no experience that indicates certain	**Low**

Risk type	Description of Risk	Risk mitigation/control	Risk assessment
		types of customers within these jurisdictions warrant a high-risk factor to be applied; however, we will continue to be vigilant.	
	The University provides opportunities to UK and international students including those from higher risk locations.	The measures adopted for student tuition fee payments, as described in the assessment of Product/Service and Customer/third party are designed to mitigate the potential risks in respect of students domiciled in high risk locations.	**Low**
Customer / third party	Most of the University's customers are UK or EEA residents. However, some students will come from and/or study in overseas, potentially higher risk locations.	Due diligence (DD) procedures have been implemented to mitigate the risk of money laundering: i) All new international students have to verify their identity at enrolment in person, for immigration purposes. ii) We do not accept cash payments. iii) Refunds are only made to the original payer of the funds and wherever possible they are made back to the same place. iv) CDD checks are performed on all sponsors, including reviewing the internet to ensure they are bona fide and credit safe checks. v) Where it is identified that an individual / third party is potentially "high risk" then sanction checks will be carried out against HM Treasury lists. These require a manual intervention; however, it is considered unlikely that an AML type risk would occur in the University's activities and any such risk would be mitigated by the routine controls. vi) We do not have any known risks associated with Politically Exposed Persons (PEPs).	**Low**

Risk type	Description of Risk	Risk mitigation/control	Risk assessment
	The University partners with overseas organisations in a variety of activities, including research and teaching. These organisations may be in potentially higher risk locations.	Other individuals and organisations (e.g. overseas agents and partners) are subject to CDD and sign legally binding agreements.	**Low**
Transaction	The University faces a number of risks associated with how we undertake business. This is particularly where it is at a distance or online which, at least in part, is becoming the norm.	Business relationships are only confirmed with international agents, partners etc. once the University has followed due process. Where the University takes on-line payments from students, they must use their student numbers and University log-on which verifies their identity before the payment is made. Students are reminded to keep their log-on details secure and not to share these with third parties. We receive reports from our payment platform provider which highlight any unusual or potential red flag payment activity. Payments from international students through the Flywire platform are subject to rigorous checks by Flywire. For distance learning courses students must complete and application process which includes submitting proof of identity and qualifications.	**Low**

Appendix 2 – High risk jurisdictions

Money Laundering and Terrorist Financing (High Risk Countries) (Amendment) Regulations 2023	**National Risk Assessment of Money Laundering and Terrorist Financing 2020 (joint HM Treasury and Home Office publication)**	**HM Treasury – list of sanctions in force in the UK** **Businesses or persons the Government directs UK businesses do not do business with**
Albania Barbados Burkina Faso Cayman Islands Democratic People's Republic of Korea (DPRK) Democratic Republic of the Congo Gibraltar Haiti Iran Jamaica Jordan Mali Mozambique Myanmar Panama Philippines Senegal South Sudan Syria Tanzania Turkey Uganda United Arab Emirates Yemen	Countries in addition to those identified in the previous column: China Hong Kong Pakistan Russia UK Crown Dependencies (i.e the Bailiwick of Jersey, the Bailiwick of Guernsey and the Isle of Man. Within the Bailiwick of Guernsey there are three separate jurisdictions: Guernsey (which includes the islands of Herm and Jethou); Alderney; and Sark UK Overseas Territories Both Crown Dependencies and Overseas Territories are viewed as high risk largely due to their lack of business ownership transparency.	UK sanctions in force

These lists are not exhaustive and only identify countries posing the highest risk. Other countries, for example, Nigeria and India are considered medium to high risk and should be viewed accordingly.

Appendix 3 Guidance Note – Examples and potential signs or red flags for money laundering

Examples

The following are examples of how suspicion of money laundering activities might arise.

Example 1

A member of staff in the course of their normal duties collects payments from international students on behalf of the University. If, before processing a transaction from a particular student, the staff member establishes the payment is being made on the student's behalf by an unrelated and / or unknown third party, then the member of staff should raise their suspicions using the process outlined in Appendix 4. They should take no further action regarding the transaction as doing so could result in the staff member committing a money laundering offence. The staff member would also commit an offence if they failed to report their suspicion and processed the transaction regardless.

Example 2

A member of staff notices a large and / or unexplained overpayment from, or on behalf of, an international student (slight foreign exchange differences are acceptable) with a request that the overpayment be returned or paid over to a third party. The staff member should report this using the process outlined in Appendix 4. They could commit a money laundering offence if they fail to report the suspicion or act on this request.

As shown by the above example, care should 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 used to make the original payment. If the staff member has any concerns or suspicions regarding the overpayment and its legitimacy this must be reported, and no further action taken.

Red Flags

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 MLNO (Money Laundering Nominated Officer). However, the following are types of risk factors and red flags which may, either alone or cumulatively with other factors, suggest the possibility of money laundering activity. If in doubt you should always report your concerns.:

- 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;
- A person or company doing business with the University that lacks proper paperwork, e.g. invoices issued by a limited company that lack details of their registered office or company number;
- Request to make a payment of a substantial sum in cash and cash transactions generally;
- Requests for payments or refunds after funds have been paid into the University's bank account by a third party, especially but not exclusively where the request is to return money to a different account or individual to the payer;
- Concerns about the honesty, integrity, identity or location of a client;
- Illogical or unusual 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;
- Where a debt to the university is settled by various third parties making a string of small payments;
- A transaction without obvious legitimate purpose or which appears uneconomic, inefficient or irrational;
- Unsolicited offers of short-term loans of large amounts, repayable by cheque or bank transfer, perhaps in a different currency and typically on the basis that the University is allowed to retain interest or otherwise retain a small sum;
- The cancellation, reversal or request for refund of an earlier transaction;
- A series of small payments made from various credit cards with no apparent connection to the student and sometimes followed by chargeback demands;
- The prospective payer asking to pay up-front a larger sum than is required or otherwise wants to make payment in advance of them being due;
- Prospective payers are obstructive, evasive or secretive when asked about their identity or the source of their funds or wealth;
- Prospective payments from a potentially risky source or a high-risk jurisdiction;
- The Payer’s ability to finance the payments required is not immediately apparent or the funding arrangements are otherwise unusual;
- 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 MLNO;
- Large donations, anonymous donations, conditions attached to donations;

- Funding for students who are the children of foreign public officials or Politically Exposed Persons and/or sanctioned individuals; and
- Students paying course fees in full and withdrawing from the course close to the start date and requesting a refund of fees.

Appendix 4 Disclosure procedure for members of staff

If you suspect that money laundering activity has taken place, or may be about to take place or if you become concerned that your involvement in a transaction may constitute money laundering, you must disclose this immediately to your line manager and do nothing further regarding the transaction until advised otherwise. If, in consultation with your line manager, reasonable suspicion is confirmed a disclosure report must be made to the MLNO.

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 MLNO directly and as soon as possible. This is important as a member of staff could prejudice the investigation of a money laundering offence if, even innocently, they notify a person who they believe may be implicated. Prejudicing an investigation is a money laundering offence in its own right..

The disclosure to the MLNO should be made on the proforma report attached at Appendix 5 and should be completed as soon as possible after the suspicion has been raised. **Should a member of staff not follow this process and fail to report their suspicion they could be personally liable to prosecution for a money laundering offence.**

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 MLNO consider the case for knowledge or suspicion of money laundering and to facilitate a SAR report to the NCA.

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

The steps taken by the MLNO on receipt of a disclosure report are outlined in a separate document (Actions to be taken by the University's MLNO on receipt of a disclosure report relating to suspected money laundering). If appropriate the MLNO will refer the case to the NCA as a Suspicious Activity Report (SAR) and the NCA will undertake any necessary investigation. This may include consent to continue with a particular transaction. Care should be taken not to 'tip off' the individuals concerned, or otherwise prejudice any investigation as this in itself can be a criminal offence.

Appendix 5 Suspected Money Laundering - Report to the MLNO

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……