Anti-Money Laundering, Terrorist Financing and Sanctions Policy		Ref: SGE0004	
Brief Description & Purpose:	This Policy outlines how the University will manage money laundering risks to ensure compliance with legislative requirements.		
Applicable to (list cohorts):	**Staff:** All staff, including Governors and co-opted Board Committee Members	**Students:** Yes	**Third Parties:** All who are in a formal relationship with the University
Effective From:	21 May 2012	**Last Review Date:**	17 March 2023
Approval Authority:	Board of Governors	**Approved:**	24 April 2023
Executive Owner:	Simon Newitt	**Business Owner:**	Tina Hannant
Next review date	March 2026	**Publication External Y/N**	Y

1. Introduction

1.1 Northumbria University is committed to 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. 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.

1.2 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.

1.3 This policy applies to all staff and students of the University and its subsidiaries as defined above, and to third parties, including academic partners undertaking business on behalf of the University.

1.4 Disciplinary action may be taken against members of staff who fail to comply with this policy.

1.5 This Policy is supported by Anti Money Laundering, Terrorist Financing and Sanctions Procedures which provide detail regarding operational procedures in place to ensure compliance.

2. Legislative and regulatory framework

2.1 The key elements of the UK Anti-Money Laundering Framework which apply to universities include:

- Proceeds of Crime Act 2002
- Terrorism Act 2000
- Counter Terrorism Act 2008
- Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017 (MLR 2017).

2.2 Money laundering is a criminal offence, with penalties including unlimited fines and/or terms of imprisonment ranging from two to fourteen years. Penalties imposed can apply to the University and to its staff as individuals, and can relate to the handling, acceptance or refunding of laundered monies. 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

2.3 The law concerning money laundering is complex and is increasingly actively enforced. It can be broken down into three main types of offences:

- the principal money laundering offences under the Proceeds of Crime Act 2002
- the prejudicing investigations offence under the Proceeds of Crime Act 2002
- offences of failing to meet the standards required of certain regulated businesses, including offences of failing to disclose suspicions of money laundering and failing to comply with the administrative requirements of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.

3. Policy Detail

3.1 Introduction to Money Laundering

3.1.1 Money laundering is the process by which the proceeds of crime are sanitised in order to disguise their illicit origins and are legitimised. Money laundering schemes come with varying levels of sophistication from the very simple to the highly complex. Straightforward 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. There are particular risks for the Higher Education sector resulting from financial transactions involving students or partners in overseas (higher risk) territories.

3.1.2 Money laundering schemes typically involve three distinct stages:

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

3.1.3 Appendix B in the Anti-Money Laundering Reporting Procedures provides examples of warning signs and potential red flags which may generate suspicions of money laundering.

3.3 The Principal Money Laundering Offences

3.3.1 These offences apply to any property (e.g., cash, bank accounts, physical property, or assets) that constitutes a person's benefit from criminal conduct or any property that, directly or indirectly, represents such a benefit (in whole or partly) where the person concerned knows or suspects that it constitutes or represents such a benefit. Any property which meets this definition is called criminal property. It is a crime, punishable by up to fourteen years imprisonment, to:

1. conceal, disguise, convert or transfer criminal property or to remove it from the United Kingdom
2. enter into an arrangement that you know or suspect makes it easier for another person to acquire, retain, use or control criminal property
3. acquire, use or possess criminal property provided that adequate consideration (i.e., proper market price) is not given for its acquisition, use or possession.

3.3.2 University staff can commit these offences when:

- handling or dealing with payments to the University;
- making or arranging to make a repayment;
- receiving donated assets on behalf of the University.

3.3.3 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.

3.3.4 Defences - In all three cases identified in 2.3.1 above, a defence may exist if a report was made to either to the Money Laundering Nominated Officer (MLNO) or the National Crime Agency (NCA) and the NCA does not refuse consent to it.

3.3.5 Failure to Disclose Offence - It is a crime, punishable by up to five years imprisonment, for a MLNO who knows or suspects money laundering or who has reasonable grounds to know or suspect it having received an authorised disclosure not to make an onward authorised disclosure to the National Crime Agency as soon as practical after they received the information.

3.3.6 The Offence of Prejudicing Investigations /Tipping-Off - The purpose of making an authorised disclosure to the National Crime Agency is to allow it to investigate the suspected money laundering so it can decide whether to refuse consent to the transaction. That investigation would be compromised if the person concerned (or indeed anyone else) were to be told that an authorised disclosure had been made. To prevent this happening, section 342 Proceeds of Crime Act 2002 provides that it is a crime, punishable by up to five years imprisonment, to make a disclosure which is likely to prejudice the money laundering investigation. University staff can commit this offence if they tell a person an authorised disclosure has been made in their case.

Authorised disclosures must be kept strictly confidential.

3.4 Terrorist Finance

3.4.1 The Principal Terrorist Finance Offences

3.4.1.1 Whereas money laundering is concerned with the process of concealing the illegal origin of the proceeds from crime, terrorist financing is concerned with the collection or provision of funds for terrorist purposes. The primary goal of terrorist financers is to hide the funding activity and the financial channels they use; the source of the funds concerned is immaterial, and it is the purpose for which the funds are intended that is crucial.

3.4.1.2 Payments or prospective payments made to or asked of the University can generate a suspicion of terrorist finance for several different reasons, but typically might involve a request for a payment, possibly disguised as a repayment or re-imbursement, to be made to an account in a jurisdiction with links to terrorism.

3.4.1.3 Sections 15 to 18 of the Terrorism Act 2000 create offences, punishable by up to fourteen years imprisonment of:

1. Raising, possessing or using funds for terrorist purposes.
2. Becoming involved in an arrangement to make funds available for the purposes of terrorism.
3. Facilitating the laundering of terrorist money (by concealment, removal, transfer or in any other way).

3.4.1.4 These offences are also committed where the person concerned knows, intends or has reasonable causes to suspect that the funds concerned will be used for a terrorist purpose. In the case of facilitating the laundering of terrorist money, it is a defence for the person accused of the crime to prove that they did not know and had no reasonable grounds to suspect that the arrangement related to terrorist property.

3.4.1.5 Section 19 of the Terrorism Act 2000 creates an offence, punishable by up to five years imprisonment, where a person received information in the course of their employment that causes them to believe or suspect that another person has committed an offence under sections 15 to 18 of the Terrorism Act 2000 and does not the report the matter either directly to the policy or otherwise in accordance with their employer's procedures.

3.5 The Offence of Prejudicing Investigations

3.5.1 Section 39 of the Terrorism Act 2000 creates an offence, punishable by up to five years imprisonment, for a person who has made a disclosure under section 19 to disclose to another person anything that is likely to prejudice the investigation resulting from that disclosure.

Disclosures made under the Terrorism Act 2000 must be kept strictly confidential.

3,6 The University's approach

3.6.1 The University adopts a risk-based approach towards Anti Money Laundering (AML) and conducting due diligence and reviews the level of risk at least every three years, or sooner where the level of risk is higher (Appendix B). Whilst many of the University's financial transactions could be considered relatively low risk from the perspective of money laundering, all staff must be vigilant against any financial crime and fraud risks that the University may face.

3.6.2 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.

3.6.3 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 them:

1. 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. The extent of due diligence required in any case will be guided by the anti-money laundering (AML) risk assessment (see 4..2 below).
2. 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.
3. Appointing a 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 5.
4. Where necessary, the MLNO reporting any suspicion of money laundering to the appropriate authorities. In the UK this is the National Crime Agency (NCA).
5. 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. 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.

3.7 The AML risk assessment

3.7.1 The University's AML controls and processes are designed to be proportionate and aligned to the risk 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.
- **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.
- **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.

3.7.2 New and emerging risks will also be considered including those identified by the National Crime Agency and other relevant sources.

3.8 Due diligence

3.8.1 The University's AML processes and controls for any transaction are designed to reflect the 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
- the geographical location / jurisdiction.

3.8.2 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. Due regard must also be given by the MLNO to the requirements of the OfS regulatory framework, as the University's principal regulator, and whether reporting is required (section 5.3 also refers).

3.8.3 Components of the University's KYC and CDD checks include:

- *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*, if there are any, 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.

3.8.4 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.

3.8.5 As there are no financial thresholds for money laundering, cash payments are a particular risk. To address this risk, the University does not universally accept cash payments.

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

3.9 Politically Exposed Persons (PEPS)

3.9.1 A politically exposed person (PEP) is someone who has 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.

3.9.2 Under anti-money laundering regulations, the main aim of applying additional scrutiny to work involving PEPs is to mitigate the risk that the proceeds of bribery and corruption may be laundered, or assets otherwise stripped from their country of origin.

3.9.3 PEPs include, but are not limited to:

- heads of state,
- heads of government, ministers, and deputy or assistant ministers
- members of Parliament
- members of courts of auditors or of the boards of central banks
- ambassadors, chargés d'affaires and high-ranking officers in the armed forces
- members of the administrative, management or supervisory bodies of state-owned enterprises
- members of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not generally subject to further appeal, except in exceptional circumstances.

3.9.4 PEPs also include:

- the person's family members
- close business associates
- beneficial owners of the person's property (someone who enjoys the benefits of ownership even though the title of the property is in another person's name)

3.9.5 The University will use information that's reasonably available to help identify PEPs, including:

- public domain information, such as parliament and government websites
- reliable public registers, such as the Companies House 'register of companies' and 'people with significant control register'
- commercial databases that contain lists of PEPs, family members and known close associates such as RiskScreen and Lexis Diligence

3.10 Financial Sanctions

3.10.1 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 will be checked, and Government guidance followed where high risk jurisdictions are involved. The UK government publishes frequently updated guidance on financial sanctions which includes a list of all targets.

The University website (LINK) is kept up to date with the latest guidance and sources of information.

3.11 Staff training and awareness

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

3.11.2 Teams identified as potentially exposed to higher risk (i.e., Advancement, GM&B, Overseas offices, Research and Innovation Services, Legal Services) are also required to complete the on-line anti-money laundering training as part of their induction process and at least every three years.

3.11.3 Completion of the mandatory training will be monitored and enforced by line managers.

3.11.3 The policy, procedures and training will be communicated and made available to all other University staff.

4. Escalation Routes Where Breach in Policy Occurs

4.1 Failure to follow the AML policy may be treated as a disciplinary matter and a breach of the Code of Conduct, particularly where the breach has exposed the University or its staff to actual or potential risk, damage or loss.

4.2 Members of the University could be committing an offence if they suspect money laundering (or if they become involved in some way) and do not report it. Examples and potential red flags are detailed in Appendix B in the supporting procedures document.

4. Roles and Responsibilities

Role	Responsibility
The Chief Financial Officer (CFO)	responsibility for the Anti Money Laundering, Terrorist Financing and Sanctions Policy, which is reviewed and approved by the Audit Committee. The CFO will ensure:

	• three yearly (more frequently if circumstances change) assessments of the University's money laundering and terrorist finance risks are conducted and relied on to ensure the effectiveness of this policy; • appropriate due diligence is conducted, as a result of which risks relating to individual transactions are assessed, mitigated and kept under review; • anti-money laundering and counter-terrorist finance training is delivered within the University, including training on this policy, with records of attendance maintained; and • this policy is kept under review and up-dated as and when necessary and levels of compliance are monitored.
Money Laundering Nominated Officer (MLNO)	primary contact for any further information or to report any suspicious activity. The MLNO is: Simon Newitt, Chief Financial Officer The Deputy MLNO is:Tina Hannant, Assistant Director Financial Control The MLNO is responsible for: • receiving reports of suspicious activity; • 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 by completing and submitting a Suspicious Activity Report; • asking the National Crime Agency for consent to continue with any transactions that must be reported and making sure that no transactions are continued illegally. Day to day responsibility and operational management shall reside with the Assistant Director, Financial Control Operational as Deputy MLNO.
All members of the University – Reporting Suspicious Activity	A student, member of staff, or governor of the University who needs to report suspicious activity **must** complete a Suspected Money Laundering report form to the MLNO as documented within the supporting procedures document. They should provide as much detail as possible and the report must be made in the strictest confidence, being careful to avoid "tipping off" those who may be involved.

5.2 Money Laundering Nominated Officer (MLNO)

The MLNO will report all relevant cases to the Head of Governance, in line with the requirements of the **Reportable Incidents Policy**. The Head of Governance will carry out any required investigations in accordance with the **Counter Fraud Policy and Response Plan** and undertake any further onward reporting.

6. Definitions

AML	Anti-Money Laundering
MLR 2017	The Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017
POCA	The Proceeds of Crime Act 2002
SAR	Suspicious Activity Report
NCA	National Crime Agency
EDD	Enhanced Due Diligence
SDD	Simplified Due Diligence
MLNO	Money Laundering Nominated Officer
PEP	Politically Exposed Person
KYC	Know Your Customer

7. Related Policies, Procedures and Other Resources

- Anti Money Laundering, Terrorist Finance and Sanctions Procedures
- Public Interest Disclosure "Whistleblowing" Policy
- Staff Code of Conduct
- Disciplinary Procedure
- Counter Fraud and Bribery Policy
- Philanthropic Gifts and Donations Policy
- Conflict of Interests Policy
- Reportable Incidents Policy
- Online Mandatory Training
- Revenue Recognition, Credit Control and Billing Policy
- National Crime Agency Suspicious Activity Reports
- Due Diligence Framework and resources
-

8. Version

Version No.	Reviewer	Date	Changes
1.0	Chris Reilly & Susan O'Donnell	26th November 2012	Revised role titles
1.1	Richard Elliott	10th October 2022	Policy format change, links added, nomenclature and role updates
1.2	Simon Newitt & Tina Hannant	February 2023	Updated to reflect legislative changes, including risk-based approach and risk assessment. Additional information added regarding Terrorist Financing Act and Sanctions. Updates to MLNO. Procedural detail removed and added to new supporting procedure document.

Appendix A

Anti-Money Laundering Risk Assessment - February 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 (HMT & Home Office joint National Risk Assessment of Money Laundering and Terrorist Financing 2020). 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.

An example of the component money laundering risk associated with payment of tuition fees is illustrated in 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
Low	EU	Parent/Guardian	International card
Medium	Non – UK or EU	Other relative	Third party/multiple payments
High	Non – UK or EU	Unrelated	International bank transfer
High	High risk jurisdictions	Unknown/suspicious and/or multiple payers	Suspicious payment patterns/cash

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. Our overseas offices and international admissions team raise student awareness and encourage them to be vigilant for attempts to draw them in to money mule activity.	Low
	Donations:	The University Philanthropic Gifts and Donations Policy contains details of the due diligence procedures to be	Low

	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.	undertaken in line with the value of the donation.	
	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 transactions.	**Low**
Jurisdiction	The University operates in both the UK and overseas territories, with some of its activities being undertaken in potentially higher risk locations. The University provides opportunities to UK and international students including those from higher risk locations.	All activities with overseas partners are subject to rigorous due diligence procedures. The University has had no experience that indicates certain types of customers within these jurisdictions warrant a high- risk factor to be applied; however, we will continue to be vigilant. 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 students must verify their identity at enrolment. 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 and performing 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.	**Low**

		vi) We do not have any known risks associated with Politically Exposed Persons (PEPs).	
	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. For distance learning courses students must complete and application process which includes submitting proof of identity and qualifications.	Low