Anti-Money Laundering (AML) Policy

Document Title: Anti-Money Laundering (AML) Policy			
Version No.	v1.1	Policy Owner	Assistant Director PS Connect (Finance)
Superseded version	November 2018	Author Role Title	Head of Financial Operations and Financial Operations Manager (AR/SFT)
Approval Date	19/03/2026	Approved by	UEB
Effective Date		Review Date	

1. Introduction

The University of Exeter is committed to upholding the highest standards of financial integrity and fully complying with UK anti-money laundering legislation, including:

- **The Proceeds of Crime Act 2002**
- **The Terrorism Act 2000**
- **The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (as amended by The Money Laundering and Terrorist (Amendment) Financing Regulations 2023)**
- **The Criminal Finances Act 2017**

This policy provides a robust framework to prevent the University from being exploited for money laundering, terrorist financing, or other financial crimes. The University's financial operations must remain transparent, accountable, and aligned with national and international compliance obligations.

The University is committed to compliance with the **Economic Crime and Corporate Transparency Act** and all associated financial regulations. Appropriate governance, financial controls, and due diligence procedures are maintained to prevent, detect, and report economic crime, including fraud and money laundering. The University ensures accurate disclosure of ownership and financial interests, supported by regular policy reviews and staff training to uphold transparency, accountability, and legal compliance.

2. Scope and Applicability

This policy applies to:

- All University staff, Council members, and associated parties (including student employees).
- University departments handling financial transactions, including Finance Services, Student Fees, Research Grants, Fundraising, and Procurement.
- External partners, donors, sponsors, research collaborators, suppliers, and agents who conduct financial dealings with the University.

3. What is Money Laundering

There are three principal money laundering offences under the Proceeds of Crime Act 2002. These offences are punishable by a maximum of 14 years imprisonment and/or a fine.

1. **Concealing**: Concealing, disguising, converting, transferring criminal property, or removing it from the UK (section 327 of the 2002 Act); or
2. **Arranging**: Entering into or becoming concerned in an arrangement which you know, or suspect facilitates the acquisition, retention use or control of criminal property by or on behalf of another person (Section 328); or
3. **Acquisition, Use, or Possession:** Acquiring, using, or possessing criminal property (section 329)

There are also two types of secondary offences:

- **Failure to Disclose**: If a staff member **suspects** money laundering but fails to report it, they may be personally liable;

- **Tipping off**: Tipping off is where someone informs a person or people who are, or who are suspected of being involved on money laundering in such a way as to reduce the likelihood of their being investigated or prejudicing and investigation.

Potentially any member of staff could be caught by the money laundering provisions if they suspect money laundering and either become involved with it in some way and/or do nothing about it.

Whilst the risk to the University of contravening the legislation is low, it is extremely important that all employees are familiar with their legal responsibilities: serious criminal sanctions may be imposed for breaches of legislation. The key requirement on employees is to promptly report any suspected money laundering activity to the Money Laundering Reporting Officer (MLRO).

4. University Responsibilities

The University must take proactive measures to mitigate financial crime risks. Key obligations include:

4.1 Risk-Based Approach

- Conducting risk assessments to identify areas vulnerable to financial crime.
- Implementing enhanced due diligence for high-risk transactions (e.g., large international payments).
- Adopting a broad cashless policy for all areas including but not limited to tuition, donations, and customer payment transactions to reduce AML risks.

4.2 Financial Controls & Due Diligence

- Ensuring Know Your Customer (KYC) checks are performed when engaging with new financial partners, donors, or suppliers.
- Verifying the identity of individuals or organisations making significant transactions.
- Monitoring unusual transactions, such as:
    - Transactions inconsistent with a party's known financial profile.
    - Multiple refunds requested in an irregular manner.

- Obligation to report suspicious activity both within the University and externally to the National Crime Agency

4.3 Staff Training & Awareness

- Annually the University will provide AML training to relevant staff, particularly within:
    - PS Connect Finance
    - Research Services
    - Exeter Innovation
    - Procurement & Fundraising
- Training will cover suspicious activity detection, reporting obligations, and regulatory updates.

4.4 Record Keeping

- All transactions, due diligence checks, and AML risk assessments will be retained for six years.
- Records must be securely stored and readily accessible for audits or regulatory inspections.

5. Employee Responsibilities

Money laundering legislation applies to ALL employees. Potentially any member of staff could be committing an offence under the money laundering laws 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 (Money Laundering Reporting Officer)

Failure to do so may result in you being personally liable to prosecution.

Employees who breach this Code of Conduct are liable for disciplinary action which may lead to their dismissal.

Guidance on how to raise any concerns is included in this policy document.

6.Identification of money laundering

All University employees must be vigilant for red flags indicating potential money laundering.

6.1 Identifying and Verifying Individuals

Before processing payments, accepting donations, or engaging in contractual arrangements, the University must confirm the legitimacy of the individual by obtaining satisfactory proof of identity, which may include:

- Students: A valid passport, visa, or birth certificate, alongside University enrolment records and correspondence to the student's permanent home address.
- Third Parties (e.g., Sponsors, Agents, or Guarantors):
    - Official letters or documents proving name, address, and relationship to the student.
    - Where applicable, direct confirmation from the student or primary sponsor.

6.2 Verifying Organisations and External Entities

For transactions involving corporate entities, donors, or external research partners, the following due diligence checks should be carried out:

- **Official Company Documentation:** Request letter-headed correspondence, a certificate of incorporation, or regulatory registration details.
- **Online Validation:** Check the company's official website, regulatory listings (e.g., Companies House for UK entities), and independent sources for legitimacy.
- **Financial Health Checks:** Request credit checks or financial statements, particularly if the organisation is unfamiliar to the University or originates from a high-risk jurisdiction.
- **Direct Contact:** Engage with key sponsors or representatives via a verified business email, phone call, or in-person meeting before finalising agreements.

6.3 Transaction Monitoring and Red Flags

Staff should exercise enhanced scrutiny where transactions exhibit unusual characteristics, such as:

- Payments made from unexpected third parties or overseas accounts not linked to the student or business.
- Unusual payment methods i.e. attempting to pay large cash deposits or cheques from unrelated sources.
- Requests for refunds to different accounts than those used for the original payment.
- Frequent changes in sponsor details or last-minute alterations to payment arrangements.

If a transaction appears suspicious, staff must escalate concerns immediately to the Money Laundering Reporting Officer (MLRO) before proceeding.

6.4 Sanctions Screening

The University will comply with all applicable sanctions legislation and will conduct appropriate due diligence to ensure that it does not engage with individuals, entities or organisations subject to sanctions. All financial transactions are screened against applicable sanctions lists, including the UK Sanctions List published by the UK Government and other relevant international sanctions regimes where required. Any identified sanctions risks will be reviewed and escalated in accordance with the University's compliance procedures.

7. Know Your Customer (KYC)

Understanding customer behaviour and transaction patterns is a critical element of the University's approach to preventing money laundering and terrorist financing. The University must ensure that all customers, whether new or existing, undergo appropriate scrutiny to assess potential risks. The following considerations help in identifying unusual activity and ensuring compliance with regulatory requirements.

7.1 New Customers

- Is verifying their identity proving difficult? Are they reluctant to provide necessary details?
- Do they have a legitimate reason for engaging with the University or its subsidiary companies?
- Are they attempting to involve intermediaries to obscure their identity or role in the transaction?
- Are they requesting large cash transactions, particularly using small-denomination notes?
- Are they requesting payment in high-denomination cash notes without a clear justification?
- Is the source of the funds known, legitimate, and reasonable?
- For international transfers or foreign currency transactions, does the explanation provided align with the business purpose and amount involved?
- Are there unusual requests regarding the collection, delivery, or method of payment?
- Have they made multiple cancellations, reversals, or refund requests in a manner inconsistent with normal activity?

7.2 Regular and Established Customers

- Is the transaction typical for the customer's usual business activity?
- Does the size and frequency of the transaction align with their established financial behaviour?

- Has there been an unexplained or significant change in the customer's transaction patterns since the relationship began?

7.3 Politically Exposed Persons (PEP)

The University recognises that Politically Exposed Persons (PEPs), their immediate family members, and close associates may present a higher risk of money laundering due to their position and influence. The organisation will take reasonable steps to identify whether a customer or beneficial owner is a PEP through due diligence and screening procedures. Where a PEP is identified, the relationship will be subject to additional scrutiny and, where appropriate, enhanced due diligence, including senior management approval and reasonable steps to establish the source of funds and wealth. Any suspicious activity must be reported to the Money Laundering Reporting Officer (MLRO), who will consider whether a Suspicious Activity Report should be submitted to the relevant authorities in accordance with applicable AML regulations.

8. What are 'reasonable grounds' for knowing or suspecting money laundering?

Under UK anti-money laundering legislation, the University has a legal obligation to disclose suspected money laundering not only when there is actual knowledge or suspicion but also when, given the circumstances, a reasonable person should have identified the risk but failed to do so.

8.1 Establishing Reasonable Grounds

Staff are expected to exercise due diligence and professional judgement when assessing financial transactions and engagements with students, customers, donors, and external partners. Reasonable grounds for suspicion may arise when:

- **Unusual Customer Behaviour:** The individual or organisation operates in a way that is inconsistent with typical dealings at the University (e.g., an unfamiliar entity offering a large donation with no clear connection to the institution).
- **Inconsistent Payment Patterns:** A student, donor, or corporate partner makes unexpected or irregular payments, such as multiple small transactions just below reporting thresholds or sudden, large transfers without explanation.
- **Third-Party Involvement:** Payments originating from an unrelated third party with no clear justification, particularly where the source of funds cannot be verified.
- **Refusal to Provide Information:** Hesitation or refusal to supply standard identity verification documents (e.g., passports, corporate registration details, financial statements) without a valid reason.
- **Complex or Opaque Transactions:** Requests for payments to be made through unusual methods, offshore accounts, or intermediary organisations without a clear business rationale.
- **Requests for Refunds to Different Accounts:** Where a payer asks for a refund to a different bank account or individual than the one originally used, especially if the refund request follows an overpayment.
- **Last-Minute Changes to Financial Arrangements:** Repeated amendments to sponsorship, donation, or tuition fee payments that lack a clear or documented reason.

8.2 Staff Responsibilities

- **Familiarity with Normal Operations:** Staff should understand the typical behaviour and expectations of students, sponsors, donors, and external organisations in their area of work.
- **Recognising Deviations from the Norm:** If a transaction or engagement differs significantly from established patterns, this may constitute reasonable grounds for suspicion.
- **Immediate Reporting:** If suspicion is aroused, staff must escalate their concerns to the Money Laundering Reporting Officer (MLRO) without delay. It is not necessary to have definitive proof—a reasonable suspicion is sufficient to require disclosure.

Failure to act on reasonable grounds may result in personal liability under anti-money laundering regulations. By remaining vigilant, staff play a critical role in protecting the University from financial crime.

9. Record Keeping Procedure

Faculties and Services conducting relevant transactions must maintain records for at least six years of:

- Student/Customer identification evidence
- Details of financial transactions carried out.

In practice, each area will routinely create and retain records in the course of normal business, and these will be sufficient for this purpose.

10. The Money Laundering Report Officer (MLRO)

The officer below is the appointed Money Laundering Reporting Officer (MLRO) for the University, and as such, receives, considers, and reports, as appropriate, on any disclosure of suspicious activities by staff.

- Dave Stacey, Chief Financial Officer

11. Disclosure Procedure

Where you know or suspect that money laundering activity is taking or has taken place, or 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 (Money Laundering Reporting Officer). This disclosure should be made on the proforma report attached in appendix 1 and should be completed the same day the information came to your attention. Should you not do so, you may be personally liable to prosecution under the money laundering regulations.

Your report should include as much detail as possible including:

- Full available details of the people, companies involved including yourself and other members of staff if relevant
- Full details of transaction 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 relevant information.

11.1 MLRO Responsibilities

The MLRO will:

- Assess the report and determine whether further investigation is required.
- If necessary, file a Suspicious Activity Report (SAR) with the UK National Crime Agency (NCA).
- Maintain confidential records of all reports received.

11.2 Confidentiality & Legal Protections

- All AML reports will be handled in strict confidence.
- Staff cannot be penalised for making a genuine AML report, even if suspicions turn out to be unfounded.

Upon receipt of a disclosure report, the MLRO must note the date of receipt and acknowledge receipt of the report. The MLRO must advise the employee of the timescale within which the MLRO will respond.To avoid committing the offence of tipping off, once reported the member of staff should not make any further enquiries into the situation, nor should they discuss their concerns with others unless instructed to do so by the MLRO.

12. Investigation

The MLRO will note and acknowledge any disclosure received and advise the individuals involved as to when a response can be expected. The MLRO will consider the report and any other available internal information he thinks relevant e.g.

- Reviewing other transaction patterns and volumes
- The length of any business relationship involved
- The number of any one-off transactions and linked one-off transaction
- Any identification evidence held.

The MLRO shall then undertake such further enquiries as necessary to investigate the matter. Inquiries will be carried out in such a way as to avoid the appearance of any tipping off of those involved.

The MLRO shall report all suspected incidents of money laundering to the competent authorities. Under the Proceeds of Crime Act, this requires a Suspicious Activity Report (SAR_ to be forwarded to the National Crime Agency:

https://www.nationalcrimeagency.gov.uk/

The MLRO shall use their discretion in deciding whether to suspend a transaction whilst any report to the competent authorities is made.

All disclosures and relevant documentation will be retained in a confidential file by the Chief Finance Officer for a minimum of six years.

Instances of suspected money laundering are likely to be rare given the nature of services provided by the University. However, we must be aware of the legislative requirements, as failure to comply would have serious implications for both the University and individuals concerned.

APPENDIX 1

Disclosure report
Internal reference number:

Suspected Money Laundering - Report to the Money Laundering Reporting Officer

From: …… Faculty / Service: ……

Contact details: ……

DETAILS OF SUSPECTED OFFENCE

Name(s) and date of Birth

Address (es) of person(s) involved including postcode

Relationship with the University.

Nature, value and timing of activity involved.

Disclosure type (nature of suspicions regarding such activity)

Provide details of any investigation undertaken to date.

Have you discussed you suspicions with anyone and if so on what basis.

Is any aspect of the transaction(s) outstanding and requiring consent to progress.

Any other relevant information that may be useful.

Signed …….. Today's date ……