University of Nottingham
UK | CHINA | MALAYSIA

Policy name	Anti-Money Laundering & Counter Terrorist Financing
Subject	The University's approach to compliance with anti-money laundering and counter-terrorist financing legislation to assist in preventing it from being used for money laundering and terrorist financing purposes
Approving authority	Assurance Committee
Accountable person	Chief Financial Officer
Responsible Team	Finance
First approved	December 2025
Last updated	December 2025
Version number	1.0

1 Introductory Purpose & Background

In recent years, Universities are at an increased risk of being used for money laundering by criminals that are creative in seeking out new opportunities. The University of Nottingham is committed to ethical standards of business and adopts a zero-tolerance approach to financial misconduct, including money laundering. Identified cases are thoroughly investigated, with sanctions applied in line with the University's disciplinary procedures. This policy outlines how the University will manage the risks of money laundering and financial crime and comply with its legal obligations in respect of:

- Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs)
- Proceeds of Crime Act 2002 (POCA)
- Terrorism Act 2000 (TA2000)
- Economic Crime and Corporate Transparency Act 2023 (ECCTA).

2 Scope

This policy applies to all University of Nottingham UK staff, particularly those who are involved in identifying students and other customers, those whose decision it is to accept students or business on behalf of the University and its UK subsidiaries. It also includes students that act as employees of the University, and associated persons, including members of Council, and covers University activities undertaken in the UK or overseas. The University's overseas campuses have their own versions of this policy.

ECCTA expanded the definition of fraud to include fraud by false representation, false accounting, fraudulent trading, cheating the public revenue, and other offenses outlined in the Fraud Act 2006 and Companies Act 2006. It also creates a criminal offence of 'failure to prevent' fraud, so that leaders and an organisation can be prosecuted for not having a suitable control environment. They do not need to be

aware of any fraudulent acts for this to apply. This fraud policy (and the mirroring documents in Malaysia and China) form the basis of that control environment.

3 Definitions

Money Laundering

Money laundering is the process by which the proceeds of criminal conduct are dealt with in a way to disguise their criminal origins. Money laundering involves three key stages:

(i) Placement: The process of getting criminal money into the financial system.
(ii) Layering: the process of moving the money within the financial system through layers of transactions.
(iii) Integration: the process whereby the money is finally integrated into the economy, perhaps in the form of a payment for a legitimate service.

Criminal property may take any form, including money or money's worth, securities, tangible property and intangible property. It also covers money, however come by, which is used to fund terrorism.

Money laundering activity includes:
(i) Acquiring, using or possessing criminal property or handling stolen goods
(ii) Handling the proceeds of crimes such as theft, fraud and tax evasion
(iii) Being knowingly involved in any way with criminal or terrorist property
(iv) Entering into arrangements to facilitate laundering of criminal or terrorist property
(v) Investing the proceeds of crimes in other financial products
(vi) Investing the proceeds of crimes through the acquisition of property/assets
(vii) Transferring criminal property.

Terrorist Financing

Terrorist financing is providing or collecting funds, from legitimate or illegitimate sources, to be used to carry out an act of terrorism with specific offences detailed under the Proceeds of Crime Act 2002 and the Terrorism Act 2000.

Associated Persons

For compliance with the ECCTA, associated persons are individuals or entities performing services for or on behalf of the University. This includes but is not limited to employees, agents, subsidiaries, consultants, volunteers, suppliers, joint venture partners and contractors.

4 Policy

4.1 Key principles

The University expects all its staff, officers, representatives and partners to follow the ethical behaviours set out in the Nolan Principles. Those are: selflessness, integrity, objectivity, accountability, openness, honesty and leadership. These Principles underpin the university's Ethical Framework and are incorporated into this policy.

The University will:

1. Conduct an annual risk assessment to identify and assess areas of risk relating to money laundering and terrorist financing particular to the University.
2. Implement controls proportionate to the risks identified.
3. Establish and maintain due diligence and guidance relating to funds received.
4. Report annually to the Assurance Committee on all aspects of this policy, including its implementation.
5. Obtain satisfactory evidence of the identity of each client with whom the University deals and/or has a business relationship, which must be retained for the duration of the relationship and for a period of five years after it terminates.
6. Report any suspicion of money laundering that is deemed appropriate to report to the appropriate authorities (HMRC).
7. Provide appropriate training via short courses or other appropriate means to all relevant members of staff where anti-money laundering and terrorist financing is relevant to their day-to-day role and to build awareness across the organisation.

4.2 Key roles, responsibilities and/or requirements

Assurance Committee are responsible for approving the University's Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Policy. They provide strategic oversight and will receive regular reports on any suspected or confirmed breaches of AML/CTF obligations, including the actions taken to mitigate future risks. This aligns with their duty to ensure the University complies with applicable legislation, including the Proceeds of Crime Act 2002 (POCA) and the Money Laundering Regulations 2017.

The Vice-Chancellor and President, as the University's Accountable Officer under the regulatory framework of the Office for Students, holds ultimate responsibility for ensuring that the University complies with its AML/CTF obligations.

Chief Financial Officer is responsible for the design and implementation of internal financial controls that support AML/CTF compliance. This includes:

- Managing AML/CTF risks within the broader University risk management framework.
- Ensuring that appropriate customer due diligence (CDD) and source of funds checks are conducted in accordance with the Partnership due Diligence Framework.
- Ensuring that the University complies with its obligations under the Money Laundering Regulations 2017, including the appointment of a Money Laundering Reporting Officer (MLRO)

Money Laundering Reporting Officer (MLRO)

The University has appointed the MLRO to assist with preventing the University from committing an offence under sections 327, 328, 329 or 342 of POCA 2002, to receive disclosures under sections 337 and 338 of POCA and to provide a single point of contact to make a disclosure to the HMRC if any member of staff is concerned that a transaction may amount to one of the money laundering or terrorist financing offences. The MLRO undertakes further training and awareness of Anti Money Laundering and Counter Terrorist Financing and ensures their understanding of the offence under section 332 of POCA. The MLRO's responsibilities are:

(i) receiving internal disclosures.
(ii) making Suspicious Activity Reports to the HMRC.
(iii) advising on anti-money laundering policies within the University; and
(iv) providing training to staff.

The Chief Financial Officer (CFO) serves as the University's Money Laundering Reporting Officer (MLRO). If a vacancy in the CFO role is anticipated, the MLRO designation will be agreed in advance through consultation with the CFO and the University Executive Board (UEB).

For December 2025 to February 2026, the Chief Governance and Risk Officer will be the interim MLRO.

All staff

All University staff must be vigilant to prevent the University from being used for money laundering and terrorist financing purposes.

Members of staff should be particularly vigilant where anti-money laundering and terrorist financing prevention is relevant to their day-to-day role. This includes staff who handle, or are responsible for handling, transactions with students, the University's clients and other third parties. All staff must carry out due diligence checks in advance including "Know Your Customer" checks in accordance with the Partnership Due Diligence framework. These checks must be undertaken for any proposed new business relationship or transaction with a person established in a sanctioned or high risk third country, or where the proposed business relationship or transaction involves a Politically Exposed Person (PEP).

Potentially any member of staff could commit an offence under money laundering legislation if they suspect money laundering and do not report it.

Failure to do so could result in staff being personally liable to prosecution.

Line managers

Line managers are expected to ensure that information regarding this policy is in induction information and that any employees for whom they have responsibility are aware of the policy.

4.3 Reporting Suspicions

If any member of staff has suspicion of money laundering or terrorist financing they must report it to the MLRO by completing the suspected Money Laundering form (appendix 2) in the Anti Money Laundering & Counter Terrorism Financing guidance. **Any suspicion must be reported. It does not have to be clear, firmly grounded or targeted on specific facts**. The report should include:

- Full details of the people, companies and staff involved including yourself and other members of staff if relevant.
- Full details of the transaction(s) (including dates, amounts, types and how they were undertaken) and the nature of each person's involvement.
- Suspected type of money laundering activity with the reasons for your suspicions.
- Any other information that may assist the MLRO to assess the transaction risk.

Once suspicions have been reported to the MLRO, staff must follow any instructions the MLRO may provide. **They must not**:

- Make any further enquiries unless they are instructed to do so by the MLRO.
- Voice their suspicions to the people they suspect of money laundering.

Where staff feel unable to report suspicions or concerns to the MLRO, staff should follow the University's Whistleblowing (Public Interest Disclosure) Code.

4.4 The consequences of non-compliance.

Failure to comply with this policy puts both individuals and the University at risk of being liable to prosecution with one potential consequence amongst others being that staff are fined or imprisoned.

Breach of this policy by any member of staff may be a disciplinary offence and staff could be subject to the University's disciplinary procedures, which could lead to disciplinary action being taken (including dismissal). Disciplinary action may be taken regardless of whether the breach of this policy is committed during working hours. Any member of staff suspected of committing a breach of this policy will be required to co-operate with the University's investigation.

4.5 How compliance with the policy will be measured.

By keeping comprehensive records, the University will be able to show that it has complied with the MLRs. This is crucial if there is a subsequent investigation into one of its customers/students or transactions.

4.6 Provisions for monitoring and reporting related to the policy.

The Partnership Due Diligence Framework ensures that the University has procedures in place for performing customer due diligence and has implemented transaction monitoring arrangements on a risk-managed basis with controls in place to mitigate money laundering and financial crime risks.

4.7 Data Protection

The University recognises that AML/CTF processes involve the collection and processing of personal data. All such processing will be conducted in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the University's Data Protection Policy.

Key data protection principles that will be adhered to throughout Anti Money Laundering /Counter Terrorist Financing processes include:

1. **Lawful, fair, and transparent processing**: The University will ensure all AML/CTF-related data processing activities are conducted under appropriate legal bases, with transparency provided to individuals where possible without compromising investigations.
2. **Purpose limitation**: Personal data collected for AML/CTF purposes will only be used for those specific purposes and not processed in a manner incompatible with those purposes.
3. **Data minimisation**: Only personal data that is necessary and relevant for AML/CTF compliance will be collected and processed.
4. **Accuracy**: The University will take reasonable steps to ensure personal data processed for AML/CTF purposes is accurate and kept up to date.
5. **Storage limitation**: Personal data will be retained for AML/CTF purposes for a minimum retention period of five years after the termination of the business relationship or transaction.
6. **Confidentiality and integrity**: Appropriate security measures will be implemented to protect personal data processed for AML/CTF purposes, with strict access controls limiting data access to authorised personnel only.

The University maintains detailed operational procedures for implementing these principles in the Records Management Policy.

5 Review

This policy will be reviewed every 2 years as a minimum.

6 Related policies, procedures, standards and guidance

Whistleblowing (Public Interest Disclosure) Code
Data Protection Policy

UK Sanctions List
Money Laundering Advisory Notice: High Risk Countries
Records Management Policy