Ethical Business: Anti-Money Laundering Policy

March 2026

POLICY

Approving authority:	Court and Audit and Risk Committee
Consultation via:	University Executive
Approval date:	26 March 2026
Review period:	Every 2 years Responsible
Executive:	University Secretary
Responsible Office:	Assurance and Legal Services
Effective date:	26 March 2026
Scope:	Global

HERIOT-WATT UNIVERSITY
Anti-Money Laundering Policy

CONTENT

1. INTRODUCTION

Heriot-Watt University ('Heriot-Watt' or 'The University') is committed to observing the provisions of anti-money laundering legislation (defined in appendix 2) in all its academic and business-related affairs at all locations. This policy supports all University staff, Court and Court Committee members at all campuses to understand and comply with relevant principles and legislation.

The University adopts a principles-based AML framework supported by customer due diligence processes to ensure integrity, transparency, and accountability in all academic, business, and financial activities.

The University's AML framework is grounded in four overarching principles:

1. Know Your Customer (KYC)
2. Source of Funds
3. Proportionality
4. Duty to Report

Customer due diligence underpins these principles, ensuring risks are assessed, identities authenticated, funds verified, and reporting duties supported.

All related policies, procedures and supporting reference documents can be found in section 13 of this policy.

For any queries on AML and/or for submission of Suspicious Activity Reports (SARs) (pro forma attached as appendix 1), please contact the Money Laundering Reporting Officer (MLRO), who serves as the University's Nominated Officer at MLRO@hw.ac.uk.

2. PURPOSE

The University has a zero-tolerance approach towards money laundering and is committed to integrity, transparency and accountability. The breaches of this policy can result in severe penalties, including imprisonment and unlimited fines for those involved, as well as significant reputational damage to the University.

3. SCOPE

This Policy applies to:

i. all University staff, Court, and Court Committee members across the Heriot-Watt Group

ii. all fee-paying students as they are customers of the University for the purposes of AML

iii. all campuses

iv. all income and expenditure

v. all University activities undertaken globally.

vi. all donors as they are 'customers' of the University for the purposes of AML

The University considers any breach of this policy as a serious matter. Failure to adhere to this policy by students and staff may result in disciplinary action, and could result in a member of staff being personally liable to criminal prosecution.

Breaches of the policy in respect of donors, who fall outside the University's disciplinary framework, may be subject to alternative actions deemed appropriate by the University, including returning donations previously made to the University. Breaches involving Court members would be considered under the University's Ordinances.

4. DEFINITION OF MONEY LAUNDERING

Money Laundering is the process by which the proceeds of crime are sanitised to legitimise them and disguise their illicit origins. 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 while the more complex schemes are likely to involve the movement of money across borders and through multiple bank accounts.

5. DEFINITION OF KNOW YOUR CUSTOMER ('KYC') AND CUSTOMER DUE DILIGENCE ('CDD')

Know Your Customer ('KYC') is a standard term used within AML frameworks globally. At the University, KYC refers to the process used to verify the identity, legitimacy, and risk profile of any individual or organisation engaging in financial activity with the University. In this context, 'customer' may include any of the following: fee-paying students, donors, partners, suppliers, sponsors, and corporate collaborators.

The University conducts Customer Due Diligence ('CDD') to verify the identity and legitimacy of individuals and organisations engaging in financial activity with the University. This may include processes to verify individuals' identities and source-of-funds verification including beneficial ownership of organisations.

Enhanced Due Diligence (EDD): EDD is performed using the 'know your donor' principles set out in the Charity Commission guidance which includes AML considerations, and is carried out using a risk-based approach. Where the risks are deemed to be higher - such as in areas where it is well known or likely that proscribed and other terrorist organisations are known to operate, the guidance requires that trustees must ensure those steps are sufficiently robust to satisfy themselves that AML and other associated risks are sufficiently addressed. In practice EDD work will be carried out by the relevant staff teams and reported to the related oversight committees and/or groups within the University, as per the applicable governance and approval processes.

EDD may include some or all of the following:

- Identity verification.
- Beneficial ownership confirmation.
- Source-of-funds review.
- Ongoing monitoring for high-risk relationships.

6. ROLES AND RESPONSIBILITIES

All staff are responsible for identifying and reporting suspicious activity. Failure to do so may lead to disciplinary and/or criminal action.

6.1 Money Laundering Reporting Officer ('MLRO')

The MLRO is the senior officer responsible for oversight of AML policy and its implementation across all global operations. At the University, this role is held by the Head of Assurance and Legal Services, or an appointed deputy in their absence.

6.2 MLRO Responsibilities

The MLRO is the only authorised individual permitted to communicate with external authorities regarding suspicious activity. To avoid tipping off, staff must not inform any person that their transactions or identity are under review.

The MLRO's responsibilities include:

- Development of the AML policy and its implementation across all campuses.
- Implementation of reporting processes for suspicious transactions or activities to relevant bodies in the jurisdictions in which the University operates.
- Receive, assess and record Suspicious Activity Reports (SARs).
- Request additional due-diligence information as needed.
- Report to:
    - National Crime Agency (UK)
    - UAE Police and FIU
    - FIED, Central Bank of Malaysia as needed.
- Halt or delay transactions pending regulatory clearance.
- Oversee AML controls, due-diligence practices and sanctions monitoring.
- Provide advice to staff and support whistleblowers.
- Deliver annual AML reporting to the Audit and Risk Committee.
- Ensure the University remains compliant with relevant global AML laws.

6.3 Other AML responsibilities

Assurance and Legal Services:

- Develop and maintain AML procedures, communication, and training.
- Ensure customer identification and due diligence processes are embedded.

Development and Alumni Office:

- The Development & Alumni Office (DAO) supports financial-crime prevention within their operational activities by carrying out proportionate due diligence on philanthropic gifts and their associated donors, consistent with the University's Charitable Gifts Acceptance Policy.
- DAO's due diligence processes includes taking reasonable steps to identify donors (using KYC principles) and, where necessary, verification of the source of funds (using EDD principles where appropriate).
- DAO assesses ethical, reputational, legal, financial, or AML-related risks associated with donations.
- All due-diligence findings are recorded in a secure log held by DAO.
- Any concerns or higher-risk cases are escalated through the appropriate University decision-making channels.
- If there are indications of potential money-laundering or financial crime, DAO will escalate the matter consistent with the AML Policy and related University reporting procedures.

Finance Team:

- Conduct appropriate verification on new suppliers and qualifying transactions using KYC/CDD/EDD principles.
- Monitor financial transactions for unusual or inconsistent activity.
- Monitor sanctions and perform sanctions screening where necessary.
- Pause transactions when risks arise.
- Maintain accurate financial records consistent with AML and University requirements.
- Support staff performing due diligence for partnerships, research collaborations, and other financial engagements by providing guidance, resources, and escalation support when risks are identified.

Global CFO:

- Ensure that the framework of financial controls, including to identify and report on AML concerns, is in place and embedded across all campuses.
- Ensure finance teams are trained and resourced.
- Managing financial-crime risks across the University in collaboration with the MLRO.
- Escalate significant AML concerns to senior management and governing bodies.

University Executive:

- Oversight of the development and implementation of the AML policy across all campuses

Audit and Risk Committee and Court**:**

- Governance and oversight of the adequacy of AML arrangements.

7. PRINCIPLES OF AML POLICY

The University's AML approach is guided by four principles, each supported by customer due diligence processes that ensure decisions are objective, risk-based and legally compliant.

7.1 Principle 1: Know Your 'Customer' ('KYC')

The University must establish and verify the identity of individuals or organisations engaging in a financial relationship with it. This may include fee-paying students, donors, partners, suppliers, sponsors, and corporate collaborators.

The level of verification required depends on the value of the transaction and the level of risk involved. Where higher risk is identified, the University must conduct proportionate Customer Due Diligence (CDD) or Enhanced Due Diligence (EDD) to confirm the identity and legitimacy of individuals and organisations transacting with it.

Customer Due Diligence may include:

- Confirmation of beneficial ownership of companies and organisations (where applicable).
- Verification of the relationship between fee-paying students and the provider(s) of their tuition fee funding.
- Enhanced Due Diligence (EDD) for Politically Exposed Persons (PEPs), high-risk jurisdictions or unusual behaviours/transactions.

Case Example: A potential research partner submits incomplete or inconsistent incorporation documents. The University pauses the due diligence process and requests the required documentation. The proposal remains on hold until satisfactory documents are provided. The case is escalated to the MLRO if the organisation submits suspicious information including presenting indicators of financial crime.

7.2 Principle 2: Source of Funds Verification

The University must ensure that incoming funds are lawful and not subject to money laundering. This includes tuition fees, sponsorships, donations, grants and corporate payments.

The extent of verification required for source-of-funds checks is determined by the transaction value and level of risk. Higher-risk payments require proportionate customer due diligence, including evidence to confirm the origin and legitimacy of funds.

Customer Due Diligence may include:

- Reviewing bank statements, payslips or income evidence.
- Requesting explanations for unusual or high-risk funds.
- Verifying the legitimacy of funding offered from charitable or corporate donors.

Case Example: A donor offers the University a potential donation of £10M but refuses to disclose the source of the funds involved. The MLRO is notified and the donation is not accepted.

7.3 Principle 3: Proportionality – Risk-Based Due Diligence

The University assesses money-laundering and terrorist financing risks associated with its activities and applies proportionate customer due diligence measures based on geographic, customer, and transactional risk factors. These controls are designed to reduce exposure to illicit funds and prevent misuse of University channels for terrorist financing.

The level of customer due diligence will be based on the level of risk and value of transactions. As risk increases, the University will undertake deeper verification, including assessing the source and legitimacy of funds and the nature of the customer relationship, and the value of the transaction. Customer due diligence also considers where funding has originated, and any risks associated with its source.

The University will scale customer due diligence measures undertaken according to the risk associated with a customer, transaction, nature, complexity, value and origin of funds and behavioural indicators.

Potential Triggers for Escalation to the MLRO:

- Third-party payments without clear justification.
- Payments from sanctioned/high-risk jurisdictions.
- Structuring or splitting payments.
- Opaque corporate/beneficial ownership of companies or organisations.

7.4 Principle 4: Duty to Report

Any staff member who identifies or suspects money laundering taking place must report the concern immediately to the MLRO. Staff are protected under whistleblowing procedures when reporting concerns in good faith, even if it turns out to be false.

8. REPORTING PROCEDURE

Court and Court Committee members and University staff must report any potentially illicit financial transactions to the MLRO. Suspicious activity may include unusual cash payments, questionable donations or inconsistent financial behaviour. Reports must be submitted securely to ensure confidentiality and protect whistleblowers.

The MLRO will review concerns, escalate serious cases and take appropriate action, which may include freezing transactions or filing a Suspicious Activity Report (SAR) with relevant regulators (e.g., NCA in the UK).

All Suspicious Activity Reports (attached as appendix 1) must be submitted to the MLRO, who serves as the University's Nominated Officer at MLRO@hw.ac.uk.

9. RECORD KEEPING

Records must be kept in accordance with the University's Information Governance and Records Management Policy and may include identity documents, transaction records, correspondence, due-diligence reports, meeting minutes, NCA reports and donor information. These records must demonstrate compliance with KYC principles and evidence of all customer interactions.

Retention requirements:

- Minimum five years after the end of the customer relationship.
- For occasional transactions: five years after transaction completion.
- For students: five years after graduation or permanent departure.
- For ongoing business relationships: records may be held up to ten years.
- For tax purposes: certain records must be retained for six years after the financial year in which the transaction occurred.

All records must be securely destroyed at the end of the retention period. The MLRO will retain SARs and associated documentation for five years.

10. COMMUNICATION AND TRAINING

The University's compliance activities support relevant staff and relevant Court and Court Committee members being made aware of the University's policies and relevant money laundering legislation. An annual programme of training for both relevant staff and for Court and Court Committee members will be undertaken to raise awareness of the policy and individual responsibilities.

The AML policy clarifies responsibilities of staff, Court and Court Committee members under the AML regime, outlines due diligence procedures and explains how to report suspicious activity. The policy is published on the University's website and communicated through internal channels.

11. MONITORING AND EVALUATION

This policy will be reviewed every two years.

The procedures associated with this policy will be reviewed annually in the light of the outcomes of the University's risk assessments and changes with Money Laundering regulations.

A report on all Ethical Business Policies (including this policy) will be submitted to the Audit and Risk Committee of Court annually. This report will provide an overview of AML legislative and policy updates, training and

awareness raising undertaken in respect of AML, and a summary of AML compliance issues reported in the year.

12. IMPLEMENTATION

The University Secretary is responsible for ensuring the effective implementation of this policy and the associated policy procedures, delegating authority as appropriate to the senior manager set out in 6 above.

The University will ensure that implementation of this policy is supported by effective procedures, guidance and appropriate generic and role-based communications, training and awareness-raising measures, applicable to all individuals and bodies referred to in the above.

13. RELATED POLICIES, PROCEDURES AND FURTHER REFERENCE

Related policies and procedures

University Financial Regulations
https://www.hw.ac.uk/document-library/financial-regulations.pdf

Ethical Business: Charitable Gifts Acceptance Policy
ethical-business-charitable-gifts-acceptance-policy

Ethical Business: Conflict of Interest Policy
Conflict of Interest Policy for Staff

Ethical Business: Gifts and Hospitality Policy
ethical-business-gifts-hospitality-policy

Ethical Business: Fraud and Bribery prevention Policy
ethical-business-fraud-bribery-prevention-policy

Modern Slavery and Human Trafficking statement
Modern-slavery-and-human-trafficking-statement

Public Interest Disclosure (Whistleblowing) Policy
public-interest-whistleblowing-policy

Information Governance and Records Management Policy
information-governance-records-management-policy

Further Reference

UK Government: Money Laundering your responsibilities
https://www.gov.uk/guidance/money-laundering-regulations-your-responsibilities

UAE Government: Combatting money laundering
https://u.ae/en/information-and-services/business/combatting-money-laundering

Central Bank of Malaysia Anti-Money Laundering / Countering Financing of Terrorism
https://amlcft.bnm.gov.my/web/amlcft

FCA: Money Laundering Regulations **https://www.fca.org.uk/firms/financial-crime/money-laundering-regulations**

National Crime Agency: Money Laundering
https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/money-laundering-and-illicit-finance

United Nations Sanctions
https://www.un.org/securitycouncil/sanctions/information

The Law Society Anti Money Laundering Sanctions guide
https://www.lawsociety.org.uk/topics/anti-money-laundering/sanctions-guide

The Charity Commission For England and Wales: Due Diligence
https://assets.publishing.service.gov.uk/media/65df4106b8da63b345c861e9/Chapter_2_Due_diligence_monitoring_and_end_use_of_funds.pdf

14. DEFINITIONS

Anti-Money Laundering (AML) Laws	Laws and regulations intended to stop criminals from disguising illegally obtained funds as legitimate income.
Customer Due Diligence (CDD)	The act of taking steps to verify the identity of new customers.
Money Laundering Reporting Officer (MLRO)	The member of staff chosen to have oversight over all activity relating to anti-money laundering.
Nominated Officer	A member of staff who must be made aware of any suspicious activity in the business that might be linked to money laundering or terrorist financing,

	and if necessary to report it. They are responsible for: • receiving reports of suspicious activity from any employee in the business • considering all reports and evaluating whether there is — or seems to be — any evidence of money laundering or terrorist financing • reporting any suspicious activity or transaction to the National Crime Agency (NCA) by completing and submitting a Suspicious Activity Report
Financial Sanctions	Financial sanctions which relate to a specific country, individual or terrorist group, known as 'regimes'. What is prohibited under each financial sanction depends on the financial sanction regulation. Regulations are imposed by the: • United Nation's Security Council – the UK is a member so automatically imposes all financial sanctions created by the UN • UK Government – a small number of financial sanctions are created by the UK Government • The Central Bank of UAE regulates AML in the UAE.
Suspicious Activity Report	A report made to the MLRO about suspicious or potentially suspicious activity which could, if necessary, be passed to the NCA for further investigation.
'Tipping off'	The offence of tipping off is committed where a person discloses that: • any person has made a report to the Police, HM Revenue and Customs or the NCA concerning money laundering, where that disclosure is likely to prejudice any investigation into the report; or • an investigation into allegations that an offence of money laundering has been committed, is being contemplated or is being carried out.
Terrorist Financing	• Terrorism financing is the act of providing financial support to terrorists or terrorist organisations to enable them to carry out terrorist acts or to benefit any terrorist or terrorist organisation. While funds may come from criminal activities, they may also be

	derived from legitimate sources, for example, through salaries, revenue from legitimate business or donations including through non-profit organisations.
Customer	• Customer may include any of the following: fee-paying students, donors, partners, suppliers, sponsors, and corporate collaborators.
Ordinance B11	• **Ordinance B11 (Removal of Members of the Court):** The University ordinance that sets out the formal process by which a member of the University Court may be removed from office. It defines the grounds, decision-making authority, and procedural steps governing the consideration of concerns relating to the conduct or suitability of Court members.
Philanthropic funds	• Voluntary donations made with charitable intent, including gifts of cash, assets, legacies, gifts-in-kind, and contributions from individuals, companies, charitable trusts, foundations, overseas governments or agencies, and similar eligible sources.

15. POLICY VERSION AND HISTORY

Version No	Date of Approval	Approving Authority	Brief Description of Amendment
VX.X	TBC	TBC	Creation of Policy

16. APPENDIX 1 – SUSPICIOUS ACTIVITY REPORT DISCLOSURE FORM

This form should be completed for all transactions which are suspected to be at risk of money laundering and should be sent as soon as possible to the Money Laundering Reporting Officer (MLRO) at legal@hw.ac.uk

Suspicious Activity Report (SAR) Disclosure Form	
Name of HW Staff member making disclosure	
HW staff email address	
Date submitted	
Third-Party details	
Name of Student/Organisation/Donor (include student id if known)	
Contact details (including email address/phone number/address as applicable)	
Transaction Details	
Please list all suspected transactions including: names, dates, card numbers, bank accounts, and amounts – as applicable:	
Please provide any further information or context below as required:	
Please provide copies of all communication with the third-party in relation to these transactions	
Have you discussed your suspicions with anyone? Yes ☐ No ☐ (If yes detail in further information below)	
Any further information to aid review	

17. APPENDIX 2 LEGISLATIVE CONTEXT

17.1 The statutory framework surrounding money laundering is centred on the following legislation:

UK

- Money Laundering, Terrorist Financing and Transfer of Funds (information on the Payer) Regulations (2017)
- Proceeds of Crime Act (2002) (UK), Part 7
- Terrorism Act (2000) (UK) (as amended by the Crime and Courts Act 2013 and the Serious Crime Act 2013)

Sanctions and Anti-Money Laundering Act (2018) (UK)

UAE

- Federal Decree Law No. 26 (2021) (United Arab Emirates)
- Cabinet Resolution No. 24 (2022) (United Arab Emirates)

Malaysia

- The Anti-Money Laundering, Anti-Terrorism Financing, and Proceeds of Unlawful Activities Act (2001) (Malaysia)

In the UK, the Primary Money Laundering Offences are set out in sections 327, 328, and 329 of the Proceeds of Crime Act 2002. These are:

- Concealing, disguising, converting, transferring criminal property with the intention of concealing or disguising their illicit source.
- Entering into or becoming concerned in an arrangement which a staff member knows or suspect facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person.
- Acquiring, using or possessing criminal property

17.2 There are further associated offences regarding due diligence and disclosures:

Due diligence

- Failure to apply customer due diligence.
- Failure to apply on-going monitoring of business relationship and customer due diligence.
- Failure to comply with timing on verification of clients and any beneficial owner.
- Failure to apply enhanced customer due diligence and monitoring where required.
- Failure to keep required records.

- Continuing with a business relationship where unable to apply customer due diligence.

Disclosures

- It is a crime, punishable by up to five years imprisonment, for a Nominated Officer, also known as the Money Laundering Reporting Officer (MLRO), 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 in the UK, and relevant local authorities should this occur in Dubai or Malaysia, as soon as practicable after receiving the information.
- University Court and Court Committee members or staff may commit a disclosure offence if they tell a person an authorised disclosure has been made in their case ("tipping off").
- University Court and Court Committee members or staff may commit a disclosure offence by failing to comply with the Public Interest Disclosure (Whistleblowing) Policy when witnessing a disclosure from Governors or staff.
- University Court and Court Committee members or staff may commit a disclosure offence if they fail to disclose.
- University Court and Court Committee members or staff may commit an offence by prejudicing an investigation due to personal reasons or failure to comply with the Conflict-of-Interest Policy.

17.3 The Proceeds of Crime Act applies to all transactions and can include dealings with agents, third parties, property or equipment, cheques, cash or bank transfers.

Money laundering regulations apply to cash transactions over 15,000 Euros (approximately £13,000). The UAE and Malaysia have their own money laundering thresholds: UAE 55,000 Dirhams and Malaysia 25,000 Malaysian Ringgits).

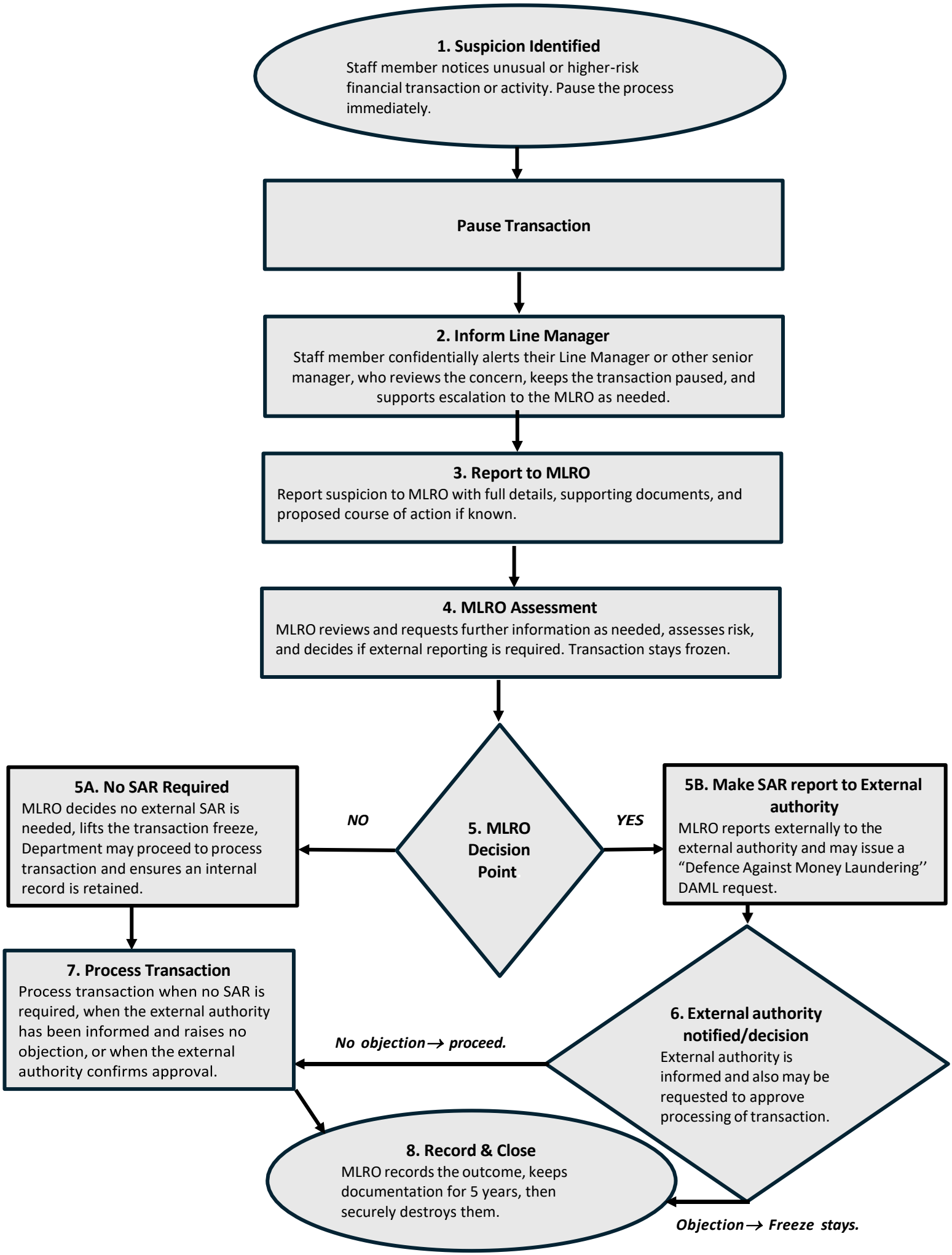
17.4 Although instances of suspected money laundering are likely to be rare, given the nature of services provided by the University, failure to comply with legal requirements could have significant implications for both the University and individuals concerned. There are specific requirements around the reporting and investigation of concerns around money laundering, and these are different for each territory within which the University operates. In the UK, suspicious activity would be reported to the National Crime Agency (NCA). In the UAE, suspicious activity would be reported to the Police and the Financial Intelligence Unit (FIU). In Malaysia suspicious activity would be notified to the Central Bank of Malaysia.

17.5 The University has a Fraud and Bribery policy which includes a Fraud Response Plan. This plan defines the authorities and responsibilities for taking action and reporting lines in the event of suspected fraud or irregularity by Court and Court Committee members, or members of staff employed by the University, temporary members of staff, contractors and

fee-paying students. If any potential cases of money laundering were detected within the University, it would be treated as potential fraud and would be investigated with under the terms of the Fraud and Bribery policy. The University Secretary will determine whether to investigate a suspected incident under the University's Disciplinary Procedure for minor cases or using the Fraud Response Plan which is intended to be used for more serious cases of suspected bribery or fraud, which includes money laundering.

17.6 Customer may include any of the following: fee-paying students, donors, partners, suppliers, sponsors, and corporate collaborators.

Appendix 2: Anti-Money Laundering (AML) reporting flowchart February 2026



Appendix 2: Anti-Money Laundering (AML) reporting flowchart February 2026

Detailed Process Guidance

Step 1. Suspicion Identified

Trigger: Any unusual, inconsistent, or higher-risk financial behaviour is detected.
Examples include:

- Unusually large payments,
- third-party payments,
- opaque or unclear sources of funds,
- unusual donor behaviour,
- sanctions concerns,
- Any activity inconsistent with the customer's expected profile

Do NOT: continue the transaction or alert ("tip off") the individual.
Action: Stop the activity immediately and record the reason for suspicion

Step 2. Inform Line Manager

Purpose: To ensure the concern is reviewed confidentially by a Line Manager or other senior manager and that the transaction remains paused before escalation to the MLRO.

Line Manager should:

- Review the concern confidentially.
- Ensure the transaction remains paused.
- Support escalation to the MLRO.

Do NOT:

- conduct your own investigation.
- discuss the concern with anyone other than your Line Manager, another senior manager, or the MLRO.

Step 3. Report to MLRO (Money Laundering Reporting Officer)

Required: All suspicious activity must be reported immediately.
How to Report:

- Submit details securely to the MLRO (via SAR Disclosure Form – see Policy, Appendix 1)
- Provide all supporting documents (e.g., emails, transaction records, identity documents).
- Clearly state any intended action (e.g., proceed, cancel, refund) with reference to existing Financial Regulations and policies.

MLRO Contact: MLRO@hw.ac.uk

Step 4. MLRO Assessment

The MLRO will:

- Acknowledge receipt of the SAR.
- Review all information and request further details if required.
- Assess risk, including:
    - source of funds,

- customer/donor identity,
- jurisdiction risks,
- sanctions matches,
- transaction patterns.

- Decide if suspicion meets the threshold for reporting to external authorities.

Throughout:

- The transaction remains frozen.
- Staff must **not** communicate with the customer or disclose that a SAR exists.

Step 5. MLRO Decision Point

Outcome 5A: No SAR to external authority Required

- MLRO concludes that the suspicion is not substantiated.
- MLRO authorises the lifting of the transaction freeze.
- The department may proceed to process the transaction in line with MLRO instructions.
- An internal record is retained for 5 years, in line with standard AML record-keeping requirements.

Outcome 5B: SAR Required (Regulated Disclosure)

- MLRO files Suspicious Activity Report externally:
  - **UK:** National Crime Agency (NCA)
  - **UAE**: Police & Financial Intelligence Unit (FIU)
  - **Malaysia**: Central Bank of Malaysia (BNM) – Financial Intelligence and Enforcement Department (FIED)
- Where needed, the MLRO may submit a Defence Against Money Laundering (DAML) request (UK context), seeking consent before proceeding with the transaction.

Step 6. External authority notified/decision

If NO objection → Proceed

- MLRO instructs the relevant department to proceed with the transaction or take an approved alternative action.

If a "MORATORIUM / HOLD NOTICE" is issued → freeze remains

- The transaction remains frozen for the statutory moratorium period.
- Staff must not contact, alert, or tip off the customer under any circumstances.

Step 7. Process Transaction

A transaction may be processed in the following circumstances:

I. No SAR Is Required

If the MLRO determines that no external SAR is required:

- The transaction freeze is lifted.
- The department may proceed to process the transaction.

Appendix 2: Anti-Money Laundering (AML) reporting flowchart February 2026

II. The external authority Is Informed (Notification Only)

If the external authority is informed for completeness and does not issue any objection:

- No hold notice is issued.
- The MLRO instructs the department to process the transaction.
- The transaction is processed as normal.

III. The external authority Confirms No Objection / Approval

If a Defence Against Money Laundering (DAML) request has been issued, then the external authority must approve the transaction:

- The freeze is lifted.
- The MLRO authorises the department to process the transaction.
- The transaction is completed in line with MLRO instructions.

Step 8. Record & Close

MLRO records must include:

- SAR details,
- Rationale for the decision taken,
- supporting documents,
- Any correspondence with external authority.

Retention Requirements:

- Minimum retention period: 5 years (standard AML requirement).
- All documents must be securely destroyed at the end of their retention lifecycle.