Anti-Money Laundering, Counter Terrorist Financing, Financial Sanction Compliance and Tax Evasion Prevention Policy

Version Control

Version	Approval Body/Officer and Date
Version 2	University Executive Board (UEB)

The full policy control and change history table is at the end of the document.

1. Purpose and Scope

This document sets out the approach taken at Cardiff University with respect to managing Money Laundering (ML), Terrorist Financing (TF), Sanction and Tax Evasion risk.

Specifically, in compliance with the following legislation:

- Terrorism Act 2000 (TA) (as amended by Anti-terrorism, Crime and Security Act 2001)
- Proceeds of Crime Act 2002 (as amended) (POCA)
- Counter-Terrorism Act 2008
- Terrorist Asset Freezing Act 2010
- Criminal Finances Act 2017
- Sanctions and Anti-Money Laundering Act 2018

Regard is paid to requirements set out within the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017) along with the content of the Joint Money Laundering Steering Group (JMLSG) guidance that sets out practical interpretation of the regulations.

As a registered charity, the guidance issued by the Charity Commission is also considered.

1.1 Applicability

This policy is applicable to all staff of the university (including those employed on a permanent, fixed term, temporary contract, or self-employed basis), students, and third parties including academic partners undertaking business on behalf of the university. It is applicable to activities completed in the UK and overseas.

Wholly owned subsidiaries may adopt this policy or establish one of their own. However, the content of any separate policy must adhere to the requirements set out in this document as a minimum.

2. Definitions

2.1 Money Laundering

Money Laundering is defined as the process by which the proceeds of crime (criminal proceeds) are made to appear to have been derived from legitimate means. Criminal proceeds may be created from a gain or the avoidance of a loss. It is also understood that criminal proceeds may not always relate to money and includes any benefit gained from criminal conduct.

The main objective of anti-money laundering (AML) controls is to understand how assets are derived along with the identification of parties involved in transactions.

2.1.1 Money Laundering process

The Money Laundering processes typically involves 3 stages:

Stage	Definition
Placement	Criminal proceeds are introduced into the financial system.
Layering	Series of actions taken with intention to disguise the true source of the criminal proceeds.
Integration	Criminal proceeds re-enter the economy appearing to be from legitimate means.

2.1.2 Principal Money Laundering Offences

The Proceeds of Crime Act (POCA) sets out offences linked to each of these stages within its principal offences. An offence is committed if involved in at least one of the stages.

POCA section	Offence
327	Concealing, disguising, converting, transferring criminal property or removing it from the UK.
328	Entering into, or becoming concerned in, an arrangement which it is known or suspected to facilitate the acquisition, retention use or control of criminal property by or on behalf of another person.
329	Acquiring, using or possessing criminal property.

POCA sets out that these offences are punishable by unlimited fines and/or imprisonment up to a maximum of 14 years, if committed.

2.1.3 Other Money Laundering Offences

In addition to the principal offences, POCA provides for 2 further offences which are applicable to the university:

POCA section	Offence
332	Failure to disclose: Nominated Officer. Committed if a Nominated Officer receives a report, investigates, and knows or suspects, or should have reason to know or suspect that an individual is involved in money laundering but fails to make a disclosure to the National Crime Agency (NCA).
342	An offence is committed where an individual who knows or suspects that a money laundering investigation is about to be or being conducted discloses information which is likely to prejudice the investigation.

As the university is not regulated, the offence of "Tipping Off" (POCA 333a) is not applicable. However, as best practice and to limit the risk of prejudicing a case, the principles of tipping off are to be recognised and considered in operational procedures and training activities.

Key definition
Tipping off is an act that alerts someone to, or discloses information on, an ongoing investigation into their financial activities by law enforcement or regulatory authorities ***and*** is likely to prejudice the investigation. The investigation information would have come to the person in the course of business in the regulated sector.

2.2 Terrorist Financing

Terrorist Financing is the raising of money by any means with the intention that the funds will be used for the purposes of terrorism or to enter arrangements to provide funds or property for that purpose.

There may be similarities in the methods used in both money laundering and terrorist financing, however, the main difference is that in addition to understanding where the funds have been generated from, the reason for their generation is also to be considered. Also, it is noted that monies gained via legitimate means may be used in terrorist financing.

Key definitions
Terrorism: an action or threat that involves violence, designed to influence the government, international governmental organisation or intimidate the public, with the purpose to advance a political, religious, racial, or ideological cause. **Terrorist/s:** an individual or group, that uses or threatens violence to influence the government or an international governmental organisation, or to intimidate the public with the pursuit of a political, religious, racial, or ideological cause.

2.2.1 Principal Terrorist Financing Offences

The Terrorism Act (TA) sets out the following offences:

TA section	Offence
15	Raising funds for terrorist purposes.
16	Possessing or intending to use funds for terrorist purposes.
17	Becoming involved in an arrangement to make funds available for the purposes of terrorism.
18	Facilitating the laundering of terrorist funds (by concealment, removal, transfer or in any other way).

2.2.2 Other Terrorist Financing Offences

In addition to the principal offences, TA provides for 2 further offences which are applicable to the university:

TA section	Offence
19	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 Terrorism Act 2000 and does not make the necessary report in accordance with this policy.

39	An offence is committed where an individual who knows or suspects that a terrorist financing investigation is about to be or is being conducted discloses information which is likely to prejudice the investigation.

2.3 Financial Sanctions

Financial sanctions are instruments used by authorised organisations with the purpose to uphold international peace and security. Financial sanctions seek to prohibit certain items, services, and/or economic resources to those targeted. Targets may be individuals, entities, sectors or entire countries.

2.3.1 Applicable regimes

Cardiff University observes and complies with financial sanctions issued by:

- United Kingdom Government (Office of Financial Sanctions Implementation – OFSI)
- United Nations Security Council (UN)
- European Union (EU)
- United States of America (Office of Foreign Assets Control - OFAC)

2.4 Tax Evasion

Tax evasion is the deliberate, dishonest attempt to not pay the tax owed to the appropriate authorities. The legal framework relating to tax evasion extends to any persons deemed to facilitate the offence by action or by failing to have adequate prevention procedures in place.

3. Policy Statements

Overarching Principles

- Cardiff University will comply with the relevant legislation (set out in 1.1) and observe the content of the Money Laundering Regulations 2017.
- Cardiff University will act ethically and with integrity in all relationships and interactions, whether academic or business related.
- Cardiff University will put in place, and monitor, proportionate systems, and controls to manage financial crime risk.
- Cardiff University will complete adequate due diligence measures on relevant parties to assess the potential financial crime risk of entering a business relationship with them. Where the financial crime risk is assessed as high, the university will put in place appropriate controls to manage this or decline/exit the relationship.
- Cardiff University will have in place suitable arrangements to escalate and thoroughly investigate any knowledge or suspicion of Money Laundering, Terrorist Financing, Sanction non-compliance or Tax Evasion.
- Cardiff University will fully cooperate with and support law enforcement or any other relevant authority with ongoing investigations in the prevention or detection of financial crime.

4. Key controls

The following controls are identified as the minimum standards by which Cardiff University manages financial crime risk. Each risk owner is required to have documented procedures in place which set out how their area of responsibility meets these requirements.

4.1 Due Diligence

Due diligence measures are essential in understanding who the university engages with, the risk associated with the relationship and the expected behaviour of the relationship. It encompasses all transactional relationships held by the university.

Risk based measures are required to be followed and documented in relation to the following relationships:

- Staff (including those employed on a permanent, fixed term, temporary contract, or self-employed basis)
- Independent members of governance bodies (Council, Board, Committees)
- Applicants / Students
- Third party payers
- Suppliers
- Partners
- Donors
- Visiting students and researchers

Due diligence measures must be completed prior to any relationship being entered into or an occasional transaction being made or received.

Key definition
Business relationship: The definition of a relationship set out within the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017) is adopted by the university - a business, professional or commercial relationship between a relevant person and a customer, which: (a) arises out of the business of the university, and (b) is expected by the university, at the time when contact is established, to have an element of duration. **Occasional transaction:** A transaction which is not carried out as part of a business relationship.

Adequate records of all due diligence activities, along with rationale on decisions made, are to be maintained in accordance with the Record Management Policy.

Due diligence information must be maintained and updated to ensure that the assessed financial crime risk of the relationship remains accurate and the appropriate controls to manage the assessed risk are in place. Ongoing review provisions are to be undertaken on a risk-based schedule and/or in response to a material change.

4.2 Sanction Screening

Risk based screening to be conducted on individuals and corporate entities that the university is proposing to enter a relationship with or is in a relationship with.

Screening activities aim to recognise any potential financial sanction exposure and to identify any proposed or existing relationships with politically exposed person (PEP) or their families and close associates.

Whilst maintaining a minimum standard across the university, risk owners can opt to increase their initial and ongoing screening criteria in recognition of the risks encountered locally. Documentation to support the approach taken is required and should be subject to regular review.

4.3 Understanding sources of funds and wealth

Fully understanding where funds originate from enables the university to assess the financial crime risk associated with a transaction. Enhanced enquiries are to be made where a transaction is unusual, or a red flag is identified. Transactions should not be processed unless the risk associated with it is understood and accepted.

Key Terms	
Source of payment (SOP)	This is where the funds are being transferred from e.g. bank account.
Source of funds (SOF)	How the specific funds being used for a transaction are derived e.g. income, savings, sale of property.
Source of wealth (SOW)	How an individual's entire wealth has been gained e.g. career, inheritance, savings.

4.3.1 Refunds

Refunds may only be processed to the account from which they originated. Any exception to this must be considered and approved by a member of senior management.

If a request is unusual or a red flag is identified, the matter should be raised with the Financial Compliance function to agree appropriate steps.

4.4 Cash Transactions

Cardiff University is a cashless organisation. Cash transactions are not permitted to be received or processed.

4.5 Ongoing Monitoring

Reactive and proactive monitoring provisions are to be in place to assess any departures from the expected behaviour or activity in a relationship. This may include but not be limited to the transactions of the relationship, the individuals involved in the relationship, or observations made when interacting with the other party.

4.6 Suspicious Activity Reporting (SAR)

POCA requires any person who knows or suspects, or has reasonable grounds to know or suspect, that a person has engaged in money laundering, to raise a Suspicious Activity Report (SAR) to the Nominated Officer. The same approach is followed at the university for knowledge or suspicion of Terrorist Financing.

Key definition
Knowledge is understood as being the sum of what is known as fact. E.g. Confirmation that a person has been charged with Money Laundering offences. Suspicion is not defined within the legislation, and therefore caselaw[1] is used to understand it. It is broadly accepted to be: • The possibility is more than fanciful if the relevant facts exist; a vague feeling of unease will not suffice; and, • The suspicion does not need to be settled in nature.

The university has appointed the Chief Financial Officer (CFO) as the Nominated Officer (NO). The Nominated Officer is permitted, under this policy, to appoint delegates to assist them with discharging their duties. Any delegate appointed will need to evidence suitable skills, knowledge, and experience to discharge the role appropriately.

A list of the current Nominated Officer and appointed delegates is detailed in appendix 3.

4.7 Training and awareness (Staff)

To meet the requirements of this policy and to enable staff to understand their individual obligations, all staff will complete mandatory training, the training will be followed by an assessment which must be successfully completed.

[1] Court of Appeal case of R v Da Silva [2006] EWCA Crim 1654

In addition to the mandatory training, role specific training will be designed and delivered to those individuals or teams deemed to have a greater responsibility for managing financial crime risk at the university.

It is important that all staff are familiar with their legal responsibilities as serious criminal sanctions may be imposed for breaches. In addition, non-compliance with this policy may constitute a disciplinary offence for staff and will be subject to investigation under the university's disciplinary procedures. This may result in disciplinary action, including dismissal.

4.8 Awareness (Students)

To protect students and limit the risk of any potential criminal proceeds being paid to the university, proactive action will be taken by the relevant departments to educate both applicants and students at the university in relation to financial crime risk.

4.9 Risk Assessment

The university is committed to putting in place appropriate, proportional, and adequate controls, that are practical, understood and adhered to, in order to manage financial crime risks. To inform the approach and target resources accordingly, a risk assessment is maintained. The risk assessment broadly follows that contained within MLR 2017 and pays regard to the following:

Risk Type	Description
Customer / Third Party	This includes staff, students, donors, suppliers, agents and any other relevant third parties.
Jurisdiction	This considers the risk presented by any connections to jurisdictions outside of the UK.
Product/Service	This considers the services offered by the university.
Transaction	This considers how and what transactions are processed by the university.
Distribution/ Channel	Assessment of the methods used by the university to enter new relationships and maintain current ones.

When conducting the assessment of money laundering, terrorist financing, sanction and tax evasion risk arising from the university's work and funding activity, the Financial Compliance function will have regard to:

- University's experiences and to any lessons learned in applying this policy.
- Guidance or assessments made by the UK government, law enforcement and regulators, including the Charity Commission, Higher Education Funding Council for Wales (HEFCW).
- Output from any other relevant organisations e.g. Financial Conduct Authority.

The content and outcome of the risk assessment will be reviewed upon any material changes and routinely on at least an annual basis. The outcome of the risk assessment may also result in changes to relevant policies.

4.10 Horizon Scanning

The financial crime landscape is ever evolving, as such relevant provisions will be in place to remain compliant and up to date with proposed changes along with intelligence issued by reliable sources. The reviews will include but not be limited to:

- New/amended legislation.
- New/updated guidance.
- Consideration of regulatory censure notices.
- Intelligence on emerging risks/trends.
- Intelligence shared by other universities or similar or relevant organisations.

An assessment of information will be conducted with any required actions recorded and tracked for completion.

5. Roles and Responsibilities

Role	Responsibility
Vice Chancellor (VC)	• Overall leadership and management of the university. • Overall financial and academic vitality of the university. • Accountable to the governing body and to government for the university's affairs. • Report externally to HEFCW any instances of serious weaknesses and fraud.
Council	• Establish Audit and Risk Committee which is responsible for providing assurance on the adequacy and effectiveness of risk management, control and governance, economy, efficiency, and effectiveness. • Responsible for the efficient management and conduct of the affairs of the university. • Sets the risk appetite for the university and puts in place structures for successful execution of the risk environment. • Report externally to Charity Commission any serious incidents. • Report externally to HEFCW breaches of Financial Management Code and/or serious failures of internal auditors.
Nominated Officer	Documentation: • Maintenance of this policy. Control framework: • Act as a focal point for all financial crime risks and issues. • Establish and maintain minimum standards and guidance to enable compliance with this policy. • Commission the annual risk assessment. Internal reporting: • Receive and investigate internal SARs received. • Onward referral to the NCA. • Maintain adequate records of all SAR investigations. External reporting: • Facilitate information to meet external reporting requirements.

	Training and awareness: • Oversight of training completion and execute controls for non-compliance. Management information: • Provide regular updates on financial compliance matters to relevant committees.
Nominated Officer Delegate	Internal reporting: • Receive and investigate internal SARs received. • Onward referral to the NCA. • Maintain adequate records of all SAR investigations.
Financial Compliance function	Control framework: • Act as the 1st point of contact for any financial compliance related queries. • Document the minimum standards and guidance to enable compliance with this policy. • Complete annual risk assessment. • Ensure continuous improvement actions are tracked and progressed when identified. Training and awareness: • Create and maintain mandatory training module. • Define, document, and deliver role specific training requirements. Management information: • Produce regular university wide updates on financial compliance matters for review and challenge.
Risk Owners	Control framework: • Ensure local procedures and processes comply with the requirements of this policy. • Where systems are utilised, ensure that system configurations comply with this policy. Training and awareness: • Ensure all staff within area of responsibility complete mandatory and assessment. • Support the creation and delivery of role specific training. Management information: • Produce relevant local updates on financial crime risk e.g. training, incidents, control improvements.
2LOD - Risk & Compliance / Assurance	Complete risk-based assurance activity to assess compliance with this policy.
3LOD - Internal Audit	Complete independent and risk-based assurance activity to assess compliance with this policy.
All staff	Internal reporting:

	• Report any knowledge or suspicion or money laundering, terrorist financing, sanction non-compliance or tax evasion to Nominated Officer. • Do not discuss any internally issued reports with any persons other than the Nominated Officer or Delegates. Control framework: • Follow compliant procedures and processes. • Escalate any potential or identified financial crime risks to line management for consideration and where required, remedial action.

6. Interaction with Law enforcement/relevant authorities

Cardiff University will interact with and assist law enforcement or relevant authorities with their investigations which relate to the prevention and detection of financial crime. This interaction will be handled initially by the Financial Compliance function and be escalated where required. The interaction will be subject to the relevant data protection provisions being in place. Adequate records of all interactions will be retained in accordance with data retentions requirements.

7. External reporting

The university is obliged to report serious incidents to the Charity Commission (CC) and/or the Higher Education Funding Council Wales (HEFCW) where reporting thresholds are met. Any reports are made in accordance with the university's Serious Incidents External Reporting Policy. In line with stated policy, the Vice Chancellor and Council delegate responsibility for external reporting to the University Secretary.

7.1 Charity Commission reporting

The requirement is to report 'any actual/alleged fraud or money laundering'. Internally, to ensure only meaningful information is shared, the following definition is used when determining whether a report is required - all confirmed fraud cases or investigations that highlight material control failures.

In addition, any links to '*terrorism or extremism, including 'proscribed' (or banned) organisations, individuals subject to an asset freeze, or kidnapping of staff'* must be reported to the Charity Commission.

7.2 Higher Education Funding Council Wales

The requirements of HEFCW delineate between fraud and Anti-Money Laundering reporting. Please see the Fraud Prevention Policy for fraud reporting requirements. In terms of non-compliance with risks covered by this policy, the requirements are to report any 'Suspicions or knowledge of Money Laundering'.

8. Management Information

To assess compliance with this policy and provide insight into the financial crime risk faced by the university, suitable Management Information (MI) will be collated, reviewed, and used to inform controls and strategies. MI will be provided to relevant stakeholders and committees to permit effective oversight and challenge.

8.1 Annual report

An annual report to be prepared and presented at least annually to the Audit and Risk Committee which will provide a high-level overview, including but not limited to:

- Comment on compliance with this policy.
- Assessment of the effectiveness of control framework.
- Evaluation of resources.
- Outcomes of second and third line of defence activities.
- Confirmation of known risks and actions plans to remedy.
- Discussion of emerging risks.
- Review risk appetite - reconfirm or amend.

9. Oversight and Monitoring

The Financial Compliance function is responsible for executing this policy and raising awareness of how to comply with it. Non-compliance with this policy carries financial, legal, and reputational penalties for both the university and its staff.

In accordance with the three lines of defence risk model, the first line owns and manages the financial crime risks within their areas of responsibility, the second line overseas risk and control compliance to provide additional assurance and the third line will provide independent assurance of the risk and control environment. Outcomes of all activities will be contained within relevant MI.

10. Data Retention

All information and documentation gained in compliance with this policy should be retained and destroyed in accordance with the university's Record Management Policy and Retention Schedules. Any personal data collected will be processed on the legal basis of processing is necessary for compliance with legal obligations.

In relation to internal decisions, adequate and sufficient rationale documentation are to be created and retained, that detail decisions made and/or risk-based approach followed. Any such documents should be accompanied by the appropriate approval in accordance with the university's governance provisions.

11. Related Policies and Procedures

This policy should be read in conjunction with:

- The Financial Regulations - Cardiff University
- Anti-Bribery Policy,
- Whistleblowing Code of Practice
- Counter-Fraud Policy
- Data Protection Policy
- Records Management Policy
- Risk Management Policy
- Serious Incidents External Reporting Policy
- Code of External Funding Practice and Serious Incident Reporting Framework.

Policy Control Information

Document Name	Anti-Money Laundering, Counter Terrorism Financing, Sanction Compliance and Tax Evasion Prevention Policy
UEB Policy Sponsor	Chief Financial Officer (CFO)
Policy Owner	Chief Financial Officer (CFO)
Policy Author(s)	Gemma Pezzack, Head of Financial Compliance
Version Number	2.0
Equality and Welsh Language Impact Assessment Date	30/04/2024
Privacy Impact Assessment Date	Not applicable – as confirmed by the Data Security Officer
Approval Date	30/04/2024
Approved By	*Vice-Chancellor (UEB)*
Date of Implementation	30/06/2024
Date of Last Review	April 2024
Date for Next Review	April 2026
For Office Use – Keywords for search function	Financial Crime, Anti-Money Laundering, AML, AML Policy, Suspicion, KYC, CDD, Money Laundering, MLRO, SAR, Nominated Officer, Counter-Terrorist Financing, Terrorist Financing, CTF, TF, Sanctions, Tax Evasion.

Change History Record

Version amended and re-viewer(s)	Description of Change	Version created
Final version by Financial Compliance Manager (Stephen Williamson)	1st version – approved by University Executive Board (UEB)	1.0 (January 2023)
1.0 amended by Head of Financial Compliance (Gemma Pezzack) to widen scope and update position on regulation.	• Clarification that Cardiff University is not regulated by the Money Laundering Regulations – however regard paid to them. • Clarification of roles and responsibilities. • The scope widened to include Counter Terrorism Financing, Sanction Compliance and Tax Evasion Prevention. • Structure aligned to Corporate Policy-making Documents Policy and Template.	2.0 (April 2024)

Appendix 1: List of Abbreviations

Abbreviation	Term
AML	Anti-Money Laundering
CC	Charity Commission
CTF	Counter-Terrorist Financing
HEFCW	Higher Education Funding Council Wales
ID&V	Identification and Verification
JMLSG	Joint Money Laundering Steering Group
MI	Management Information
ML	Money Laundering
MLR	The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations
NCA	National Crime Agency
NO	Nominated Officer
NOD	Nominated Officer Delegate
POCA	Proceeds of Crime Act 2002 (as amended)
Regs	The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations
SAR	Suspicious Activity Report
TA	Terrorism Act 2000 (as amended)
TF	Terrorist Financing

Appendix 2: Suspicious Activity Report (SAR)

Suspicious Activity Report (SAR)

About you			
Reporter name		Reporter team	
Reporter email address		Reporter telephone contact	
School/College/Service		Date of report	
About suspicion			
Name			
Address			
Unique identifier			
Relationship type (student/donor/supplier)			
Reason for suspicion			
Guidance: Please provide as much detail as possible in relation to why you formed your suspicion, specific actions, behaviours, transactions involved.			
Supporting information and/or documentation			
Guidance: Please detail information and documentation reviewed when considering whether the action is suspicious along with details of any further actions taken in response to this matter. Please attach any supporting documentation.			
Have you spoken to anyone regarding this matter? If yes, who?			
Guidance: If a transaction or behaviour is unusual, guidance may be sought initially from direct line manager/team, however when a suspicion is formed – the matter should only be discussed with the Nominated Officer/Delegates.			

Red flags

- Proposed payments in cash.
- Overpayments / accelerated payments for no obvious reason.
- Request for refunds that are unusual or requested to return to a different account.
- Payments from seemingly unrelated / multiple third parties.
- Payment for course early and withdrawing before start date.
- Overly complicated structure.
- Unable or, payer unwilling, to confirm SOF/SOW.
- Payments from multiple sources.
- Low payments on card (testing controls).

Supporting steps

- Consider CDD information held, where required, update CDD information.
- Review previous activity / transactions on account.
- Make enquiries in relation to payment e.g., if third party, the name on the account.
- Make general queries with individual (notwithstanding tipping off risk).

Report

- Complete and submit an Internal Suspicious Activity Report (this form).
- Email report to Suspiciousactivityreporting@cardiff.ac.uk.
- Do not discuss your suspicions with anyone. These may ONLY be discussed with the Nominated Officer or a delegate.
- If immediate advice required - contact the Financial Compliance team and flag this contact as urgent.

Nominated Officer:
- Darren Xiberras (CFO)

Delegates:
- Natalie Stewart (Group Financial Controller)
- Helen Bennett (Head of Financial Compliance)

TO BE COMPLETED BY NOMINATED OFFICER OR DELEGATE ONLY

Background
Investigation
Conclusion

Administration			
Investigator		SAR reference	
Investigation commenced		Investigation concluded	
Referred to NCA	Y/N	NCA code/s	
DAML required	Y/N	DAML received	Y/N

Appendix 3: Nominated Officer and Delegates

Role	Name	Job title	Effective date
Nominated Officer	Darren Xiberras	Chief Financial Officer	March 2023
Delegate	Natalie Stewart	Group Financial Controller	November 2023
Delegate	Gemma Pezzack	Head of Financial Compliance	November 2023

Appendix 4: Indicators of high-risk transactions or relationships (red flags)

The below provides examples of activity which present an increased risk on non-compliance with financial crime legislation.

General:

- Proposed payments in cash.
- Overpayments / Payments made ahead of schedule with no obvious reason why.
- Request for refunds that are unusual or requested to return to a different account.
- Payments from seemingly unrelated / multiple third parties.
- Payment for course early and withdrawing before start date.
- Overly complicated corporate structures.
- Unable or, payer unwilling, to confirm Source of Funds/Source of Wealth.
- Payments from multiple sources.
- Low payments on card (testing controls).
- Payments originating from high-risk jurisdictions.
- Same address and/or contact details as another individual/entity with no plausible explanation.

Suppliers specific:

- Potential or existing supplier submits a very low quotation or tender.

Donations specific:

- Conditions attached to donations.
- University asked to act as conduit to pass funds from one person to another.
- Timing of donation / payment is unusual.

Appendix 5: Management Information (MI)

Monthly MI

Management information (MI) to be provided to the Nominated Officer and shared among the Delegates and Financial Compliance function regularly. This MI should detail, but not be limited to:

- Investigation updates/outcomes
- Function performance and resource
- Changes to risks assessments/control frameworks
- Details of emerging risks
- Details of reactive and proactive ongoing projects

Audit and Risk Committee

MI for the review period will be collated and presented at the Audit and Risk Committee for consideration when it sits. This will be a culmination of the monthly MI created for the Nominated Officer.