Anti-Money Laundering Policy – Guidance Document

Introduction

Cardiff University is committed to observing the provisions of the Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017, the Proceeds of Crime Act 2002, Part 7 – Money Laundering Offences and the Terrorism Act 2000 (as amended by the Crime and Courts Act 2013 and the Serious Crime Act 2013) in all its affairs, whether academic or business related. This policy aims to ensure that Cardiff University and all its employees comply with the legislation and that due diligence is applied in relation to 'know your customer' principles.

This policy sets out the procedure to be followed if money laundering is suspected and defines the responsibility of individual employees in the process.

Cardiff University has a zero-tolerance policy towards money laundering, and is committed to the highest level of openness, integrity, and accountability, both in letter and in spirit. The penalties for these offences are severe and can mean up to 14 years imprisonment and/or an unlimited fine for the employees and executives responsible. In addition, there would be significant reputational damage for Cardiff University.

What Is Money Laundering?

Money laundering is the process of taking profits from crime and corruption and transforming them into legitimate assets. It takes criminally derived 'dirty funds' and converts them into other assets so they can be reintroduced into legitimate commerce. This process conceals the true origin or ownership of the funds, and so 'cleans' them.

Placement - movement of criminal property from their source. For example, cash proceeds from crime may be paid into a bank or used to buy goods, property, or assets.

Layering - undertaking transactions to conceal the origin of the criminal property. For example, goods or other assets may be resold or funds transferred abroad. This distances the criminal property from its illegal source.

Integration - movement of criminal property into the legitimate economy so that it looks as if this came from lawful sources

Most anti-money laundering laws that regulate financial systems link money laundering (which is concerned with source of funds) with terrorism financing (which is concerned with destination of funds).

In practice, an ostensibly legitimate and regular transaction - such as the payment of student fees and their subsequent refund - can disguise money laundering and it is essential that universities deploy a range of risk-based policies and procedures to ensure that they do not become involved in money laundering by inadvertently legitimising suspect individuals or transactions.

UK legislative and regulatory framework

In the UK, severe penalties are imposed on individuals connected with any stage of laundering money. Penalties include unlimited fines and/or terms of imprisonment ranging from 2 to 14 years.

Money laundering offences include:

(i) *the "concealing" offence:* concealing, disguising, converting, and/or transferring criminal property or removing it from the UK; (Section 327 of the Proceeds of Crime Act 2002 (POCA))

(ii) *the "arranging" offence:* 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, POCA)

(iii) *the "acquisition, use and possession" offence:* acquiring, using or possessing the proceeds of crime (Section 329, POCA)

(iv) Making a disclosure to a person which is likely to prejudice a money laundering investigation ("tipping off") (Section 333, POCA)

(v) Becoming concerned in an arrangement facilitating concealment, removal from the jurisdiction, transfer to nominees or any other retention or control of terrorist property (Section 18, Terrorist Act 2000)

The first three offences listed above require either "knowledge or suspicion" of criminal conduct. A suspicion does not have to be clear or firmly grounded, or supported by evidence, provided it is a possibility which is more than fanciful – this is a very low bar to cross. It is also an offence to **fail to report** knowledge or suspicion of money laundering. An offence can also be committed by **prejudicing an investigation** into money laundering.

There is no minimum financial threshold for money laundering offences, they can apply to money laundering involving any amount. There are also no limitation periods within which a prosecution must be brought. UK money laundering offences can be committed even where the proceeds of crime relate to criminal conduct which occurred abroad.

Key elements of the UK Anti-Money Laundering framework that apply to Cardiff University include:

- Proceeds of Crime Act 2002 (as amended)
- Terrorism Act 2000 (as amended by the Anti-terrorism, Crime and Security Act 2001)
- Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017)
- Counter-terrorism Act 2008, Schedule 7
- HM Treasury Sanctions Notices and News Releases
- Joint Money Laundering Steering Group (JMLSG) Guidance.

Risk Assessment

The Joint Money Laundering Steering Group (JMLSG) which is a highly regarded private sector body that is made up of the leading UK Trade Associations in the financial services industry and the Financial Conduct Authority (FCA) which regulates the financial services industry in the UK Financial Crime Guidance provide advice for assessing money laundering risks associated with these risk headings, and what activities may increase those risks. Typically, these would include:

- **Product/Service and Distribution** Cash transactions, anonymous transactions, non-face-to-face transactions, transactions involving unknown third parties and unregulated transactions (i.e. from unregulated third-parties)

- **Customer/Third-Party** Unusual business relationships, cash businesses, non-UK /non-local residents and Politically Exposed Persons (PEP's) and Sanctioned Parties

- **Country, geographic and jurisdictional** Countries recognised to have inadequate AML/CTF controls and processes, countries subject to sanctions, embargoes and related measures and countries identified by recognised authorities as supporting terrorism and/or terrorist organisations. A list of high-risk countries can be found at https://www.cardiff.ac.uk/__data/assets/excel_doc/0003/2702172/High-Risk-Country-List.xlsx

- **Distribution** Risks associated with how we undertake business, including direct and indirect relationships (e.g. via an agent or third-party), face-to-face, digital/online and telephonic.

Further details of these organisations' guidance can be found at:

JMLSG - https://www.jmlsg.org.uk/guidance/current-guidance/

FCA- https://www.handbook.fca.org.uk/handbook/FCG.pdf

Possible signs of money laundering include:

i) large cash payments;
ii) multiple small cash payments to meet a single payment obligation;
iii) payments or prospective payments from third parties, particularly where
    i. there is no logical connection between the third party and the student, or
    ii. where the third party is not otherwise known to the University, or
    iii. where a debt to the university is settled by various third parties making a string of small payments;
iv) payments from third parties who are foreign public officials or who are politically exposed persons ("PEP");
v) payments made in an unusual or complex way;
i) unsolicited offers of short-term loans of large amounts, repayable by cheque or bank transfer, perhaps in a different currency and typically on the basis that the University is allowed to retain interest or otherwise retain a small sum;
ii) donations which are conditional on particular individuals or organisations, who are unfamiliar to the University, being engaged to carry out work;
iii) requests for refunds of advance payments, particularly where the University is asked to make the refund payment to someone other than the original payer;

iv) a series of small payments made from various credit cards with no apparent connection to the student and sometimes followed by chargeback demands;
v) the prospective payer wants to pay up-front a larger sum than is required or otherwise wants to make payment in advance of them being due;
vi) prospective payers are obstructive, evasive or secretive when asked about their identity or the source of their funds or wealth;
vii) prospective payments from a potentially risky source or a high-risk jurisdiction;
viii) the payer's ability to finance the payments required is not immediately apparent or the funding arrangements are otherwise unusual.

5.8 The process considers each of the above risk factors and rates them on a RAG (Red, Amber, Green) scale equating to High, Medium and Low.

KYC and CDD Principles

Customer Due Diligence (CDD) is part of Know Your Customer (KYC) because KYC is the due diligence that universities must perform in order to identify their business relationships and customers and, hence, ascertain relevant information pertinent to doing financial business with them

Undertaking KYC and CDD not only ensures that a university complies with the law, but it also makes good business sense by helping to ensure that a university does not enter into any relationships that might be considered too risky.

There are essentially three components that make up the CDD measures required by the Money Laundering Regulations. The three components are:

1. Ascertaining and verifying the identity of the customer/student i.e. knowing who they are and confirming that their identity is valid by obtaining documents or other information from sources which are independent and reliable. For the most part, to satisfy the requirements identity checks for money laundering purposes are interpreted as obtaining a copy of photo-identification (such as a passport) and proof of address (such as a recent utility bill).

2. Ascertaining and verifying (if appropriate) the identity of the beneficial owners of a business, if there are any, so that you know the identity of the ultimate owners or controllers of the business.

3. Information on the purpose and intended nature of the business relationship i.e. knowing what you are going to do with/for them and why.

There are three levels of CDD – 'Standard', 'Simplified', and 'Enhanced'.

<u>Standard due diligence (CDD)</u>

In most cases, standard due diligence is the level of due diligence that will be used. These are generally situations with a potential risk, but it is unlikely that these risks will be realised.

Standard due diligence requires you to identify your customer as well as verify their identity. Besides, gathering information is required to understand the nature of the business

relationship. This due diligence should provide you with confidence that you know who your customer is and that your service or product is not being used as a tool to launder money or any other criminal activity.

Simplified due diligence (SDD)

Simplified due diligence is permitted where you determine that the business relationship or transaction presents a low risk of money laundering or terrorist financing, taking into account your risk assessment.

Regulation 37(3) sets out a list of factors to be taken into account in determining whether a situation poses a lower risk of money laundering or terrorist financing, such that SDD measures can be applied.

Enhanced due diligence (EDD)

Enhanced customer due diligence and monitoring (EDD) is required by the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017) in any situation where there is a higher risk of money laundering or terrorist financing.

Regulation 33(1) sets out a list of circumstances in which EDD measures must be applied. It includes any transaction or business relationship involving:

i) a person established in a "high-risk third country" https://www.cardiff.ac.uk/__data/assets/excel_doc/0003/2702172/High-Risk-Country-List.xlsx
ii) any transaction or business relationship involving a "Politically Exposed Person" (PEP) or a family member or known associate of a PEP
iii) any other situation that presents a higher risk of money laundering or terrorist financing

The University should ensure the CDD records relied on are retained for five years from the date on which reliance commences. Failure to do so is a criminal offence.

Politically Exposed Persons (PEP's)

Definition

Regulation 35 defines PEP's as A PEP is defined as an individual who is entrusted with prominent public functions, other than as a middle-ranking or more junior official.

Individuals who have, or have had, a high political profile, or hold, or have held, public office, can pose a higher money laundering risk to firms as their position may make them vulnerable to corruption. This risk also extends to members of their immediate families and to known close associates. PEP status itself does not, of course, incriminate individuals or entities. It does, however, put the customer, or the beneficial owner, into a higher risk category. The level of risk associated with any PEP, family member or close associate (and the extent of EDD measures to be applied) must be considered on a case-by-case basis.

Individuals entrusted with prominent public functions include:

- heads of state, heads of government, ministers and deputy or assistant ministers;
- members of parliaments or of similar legislative bodies;
- members of supreme courts, of constitutional courts or of other high-level judicial bodies the decisions of which are not subject to further appeal, except in exceptional circumstances;
- members of courts of auditors or of the boards of central banks;
- ambassadors, charges d'affaires and high-ranking officers in the armed forces (other than in respect of relevant positions at Community and international level);
- members of the administrative, management or supervisory boards of State-owned enterprises; and
- directors, deputy directors and members of the board or equivalent function of an international organisation.
- These categories do not include middle-ranking or more junior officials.

Regulation 35(9) confirms that under the definition of a PEP the obligation to apply EDD measures to an individual ceases after they have left office for one year, or for such longer period as the firm considers appropriate, in order to address risks of ML/TF in relation to that person.

Associated PEP's

Family members of a PEP include:

- a spouse or partner of that person;
- children of that person and their spouses or partners; and
- parents of that person.

Known close associates of a PEP include:

- an individual who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with a PEP; and
- an individual who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of a PEP.

A firm is no longer obliged to apply EDD measures to family members or close associates of a PEP when the PEP is no longer entrusted with a prominent public function, whether or not the period in Regulation 35(9) has expired.

Regulation 35(15) states that for the purpose of deciding whether a person is known to be a close associate of a PEP, the firm need only have regard to any information which is in its possession, or which is publicly known. Having to obtain knowledge of such a relationship does not presuppose active research by the firm.

Source of wealth

Regulation 35(5)(b) states that firms must take adequate measures to establish the source of wealth and source of funds which are involved in the business relationship in order to allow the firm to satisfy itself that it does not handle the proceeds from corruption or other criminal activity.

The measures University departments should take to establish the PEP's source of wealth and the source of funds will depend on the degree of risk associated with the business relationship, and where the individual sits on the PEP continuum. University departments should verify the source of wealth and the source of funds based on reliable and independent data, documents, or information where the risk associated with the PEP relationship is particularly high.

Senior management approval

When seeking to obtain approval for establishing, or continuing, a business relationship with a PEP, family member of a PEP or close associate, approval must be provided by the relevant head of department. Where a head of department is seeking approval, they must obtain that approval from an authority at least one grade higher than themselves.

On-going monitoring

New and existing customers may not initially meet the definition of a PEP but may subsequently become one during the course of a business relationship. The relevant department heads should, as far as practicable, instigate operating processes that are alert to public information relating to possible changes in the status of its customers with regard to political exposure. When an existing customer is identified as a PEP, EDD measures must be applied to that customer.

Suspected Money laundering Reporting Form

CONFIDENTIAL - Suspected Money Laundering Reporting Form Please complete and send this by email to the MLRO using the details below	
From:	School/College/Service
Contact Details:	
DETAILS OF SUSPECTED OFFENCE [Please continue on a separate sheet if necessary]	
Name(s) and address(es) of person(s) involved, including relationship with the University:	
Nature, value and timing of activity involved:	
Nature of suspicions regarding such activity:	

Details of any enquiries you may have undertaken to date:	
Have you discussed your 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:	Date:
Please do not discuss the content of this report with anyone you believe to be involved in the suspected money laundering activity described. To do so may constitute a tipping off offence.	

Once complete please email to: financialcompliance@cardiff.ac.uk