Customer Fraud Anti Money Laundering Procedure

Version – v1 – February 2023

Procedure Author – Head of Finance

Procedure Owner – Vice Principal, Finance and Infrastructure

Parent Policy Statement – Finance Policy Statement

Public Access or Staff Only Access – Public

Version – Version 1 – February 2023

Changes and Reason for Changes – New Procedure

CUSTOMER FRAUD ANTI MONEY LAUNDERING PROCEDURE

Introduction

Purpose

1. The University is committed to ensuring the highest standards of probity in all of its financial dealings. It will therefore ensure that it has in place proper, robust financial controls so that it can protect its funds and ensure continuing public trust and confidence in it. Some of those controls are intended to ensure that the University complies in full with its obligations not to engage or otherwise be implicated in money laundering or terrorist financing. This Procedure sets out those obligations, the University's response and the processes to be followed to ensure compliance.

Implementation

2. The Vice Principal (Finance and Infrastructure) is directly responsible to the Court of the University for safeguarding the institution from financial fraud and implementation of a duty of care to students undertaking financial transactions with UWS. As such, they will ensure:

   i) regular assessments of the University's money laundering and terrorist finance risks are conducted and relied on to ensure the effectiveness of this Procedure;

   ii) appropriate due diligence is conducted, as a result of which risks relating to individual transactions are assessed, mitigated and kept under review;

   iii) anti-money laundering and counter-terrorist finance training is delivered within the University, including training on this Procedure; and

   iv) that this Procedure is kept under review and up-dated as and when necessary and levels of compliance are monitored.

3. Certain functions under this Procedure are to be undertaken by a Nominated Officer. For the purposes of this Procedure, the Nominated Officer is the Head of Finance and, in their absence, the Lead Finance Business Partner or the Financial Controller.

4. This Procedure applies to all staff who are engaged in financial transactions for or on behalf of the University. Any failures to adhere to this Procedure may be dealt with

under the University's disciplinary or performance management procedures, as appropriate. Note that any such failures also expose the individual concerned to the risk of committing a money laundering offence.

What is Money Laundering?

5. Money laundering is the process by which the proceeds of crime are sanitised in order to disguise their illicit origins and are legitimised. 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 whilst the more complex schemes are likely to involve the movements of money across borders and through multiple bank accounts. Money laundering schemes typically involve three distinct 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; and

   iii) integration – the process whereby the money is finally integrated into the economy, perhaps in the form of a payment for a legitimate service.

Money Laundering Warning Signs or Red Flags

6. Payments or prospective payments made to or asked of the University can generate a **suspicion** of money laundering for a number of different reasons. For example:

   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

      a. there is no logical connection between the third party and the student, or

      b. where the third party is not otherwise known to the University, or

      c. 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;

vi) 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;

vii) donations which are conditional on particular individuals or organisations, who are unfamiliar to the University, being engaged to carry out work;

viii) requests for refunds of advance payments, particularly where the University is asked to make the refund payment to someone other than the original payer;

ix) a series of small payments made from various credit cards with no apparent connection to the student and sometimes followed by chargeback demands;

x) 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;

xi) prospective payers are obstructive, evasive or secretive when asked about their identity or the source of their funds or wealth;

xii) prospective payments from a potentially risky source or a high-risk jurisdiction;

xiii) the payer's ability to finance the payments required is not immediately apparent or the funding arrangements are otherwise unusual.

Money Laundering - The Law

7. The law concerning money laundering is complex and is increasingly actively enforced. It can be broken down into three main types of offences:

i) the principal money laundering offences under the Proceeds of Crime Act 2002;

ii) the prejudicing investigations offence under the Proceeds of Crime Act 2002; and

iii) offences of failing to meet the standards required of certain regulated businesses, including offences of failing to disclose suspicions of money laundering and failing to comply with the administrative requirements of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.

The Principal Money Laundering Offences

8. These offences, contained in sections 327, 328 and 329 Proceeds of Crime Act 2002, apply to any property (e.g. cash, bank accounts, physical property, or assets) that constitutes a person's benefit from criminal conduct or any property that, directly or indirectly, represents such a benefit (in whole or partly) where the person concerned knows or suspects that it constitutes or represents such a benefit. Any property which meets this definition is called criminal property. It is a crime, punishable by up to fourteen years imprisonment, to:

   i) conceal, disguise, convert or transfer criminal property or to remove it from the United Kingdom;

   ii) enter into an arrangement that you know or suspect makes it easier for another person to acquire, retain, use or control criminal property; and

   iii) acquire, use or possess criminal property provided that adequate consideration (i.e. proper market price) is not given for its acquisition, use or possession.

9. University staff can commit these offences when handling or dealing with payments to the University: if they make or arrange to make a repayment, they risk committing the first two offences, and if they accept a payment, they risk committing the third offence.

Defences

10. In all three cases, they will have a defence if they made a so-called *authorised disclosure* of the transaction either to the Nominated Officer or to National Crime Agency and the National Crime Agency does not refuse consent to it.

Failure to Disclose Offence

11. It is a crime, punishable by up to five years imprisonment, for a Nominated Officer 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 as soon as practicable after they received the information.

12. At paragraph 31 below, this Procedure sets out how such disclosures are to be made.

The Offence of Prejudicing Investigations / Tipping-Off

13. The purpose of making an authorised disclosure to the National Crime Agency is to allow it to investigate the suspected money laundering so it can decide whether to refuse consent to the transaction. That investigation would be compromised if the person concerned (or indeed anyone else) were to be told that an authorised disclosure had been made. To prevent this happening section 342 Proceeds of Crime Act 2002 provides that it is a crime, punishable by up to five years imprisonment, to make a disclosure which is likely to prejudice the money laundering investigation. University staff can commit this offence if they tell a person an authorised disclosure has been made in their case. At paragraph 34 below, this Procedure requires authorised disclosures to be kept strictly confidential.

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017

14. These regulations are aimed at protecting the gateway into the financial system. They apply to a range of businesses all of which stand at that gateway. They require these businesses to conduct money laundering risk assessments and to establish policies and procedures to manage those risks. Businesses to which the regulations apply are specifically required to conduct due diligence of new customers, a process known as “Know your Customer” or “KYC”. There are criminal sanctions, including terms of imprisonment of up to two years, for non-compliance. Whilst the University is not covered by the regulations in its work as a provider of education, the regulations provide a guide to the management of risk in handling money and due diligence is at the heart of the University’s approach in this Procedure to managing risk.

Terrorist Finance

The Principal Terrorist Finance Offences

15. Whereas money laundering is concerned with the process of concealing the illegal origin of the proceeds from crime, terrorist financing is concerned with the collection or provision of funds for terrorist purposes. The primary goal of terrorist financers is to hide the funding activity and the financial channels they use. Here, therefore, the source of the funds concerned is immaterial, and it is the purpose for which the funds

are intended that is crucial.

16. Payments or prospective payments made to or asked of the University can generate a suspicion of terrorist finance for a number of different reasons, but typically might involve a request for a payment, possibly disguised as a repayment or re-imbursement, to be made to an account in a jurisdiction with links to terrorism.

17. Sections 15 to 18 Terrorism Act 2000 create offences, punishable by up to 14 years imprisonment, of:

    i) raising, possessing or using funds for terrorist purposes;

    ii) becoming involved in an arrangement to make funds available for the purposes of terrorism; and

    iii) facilitating the laundering of terrorist money (by concealment, removal, transfer or in any other way).

18. These offences are also committed where the person concerned knows, intends or has reasonable cause to suspect that the funds concerned will be used for a terrorist purpose.

19. In the case of facilitating the laundering of terrorist money, it is a defence for the person accused of the crime to prove that they did not know and had no reasonable grounds to suspect that the arrangement related to terrorist property.

20. Section 19 Terrorism Act 2000 creates an offence, punishable by up to five years imprisonment, where a person receives 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 then report the matter either directly to the police or otherwise in accordance with their employer's procedures. This Procedure sets out those procedures at paragraph 32 below.

The Offence of Prejudicing Investigations

21. Section 39 Terrorism Act 2000 creates an offence, punishable by up to five years imprisonment, for a person who has made a disclosure under section 19 Terrorism Act 2000 to disclose to another person anything that is likely to prejudice the investigation resulting from that disclosure. At paragraph 34 below, this Procedure requires disclosures under the Terrorism Act 2000 to be kept strictly confidential.

OUR PROCEDURES

Overview

22. Under the leadership of the Nominated Officer, the University will:

i) conduct an annual risk assessment to identify and assess areas of risk money laundering and terrorist financing particular to the University;

ii) implement controls proportionate to the risks identified;

iii) establish and maintain procedures to conduct due diligence on funds received;

iv) review procedures annually and carry out on-going monitoring of compliance with them;

v) appoint a Nominated Officer to be responsible for reporting any suspicious transactions to the National Crime Agency;

vi) provide training to all relevant members of staff, including temporary staff, on joining the University, and provide annual refresher training; and

vii) maintain and retain full records of work done pursuant to this Procedure.

The University's Risk Assessment, Continuous Review and Accountability

23. At least once a year, and more frequently if there is a major change in circumstances, the Vice Principal (Finance and Infrastructure) will:

i) conduct an assessment of money laundering and terrorist finance risk in the University's work;

ii) review and, if necessary, revise this Procedure in light of that risk assessment;

iii) review and, if necessary, revise the University's arrangements for ensuring compliance with this Procedure so that resources are targeted to the areas of greatest risk; and

iv) report to the Court of the University on all aspects of this Procedure, including its implementation.

v) In order to facilitate the review and accountability functions, the Vice Principal (Finance and Infrastructure) will ensure: the availability of appropriate management information to permit effective oversight and challenge; and

vi) the maintenance and retention of full records of work done under this

Procedure.

24. In conducting the assessment of money laundering and terrorist financing risk arising from the University's work and funding activity, the Vice Principal (Finance and Infrastructure) will have regard to the University's experiences and to any lessons learned in applying this Procedure. They will also take into account any guidance or assessments made by the UK government, law enforcement and regulators, including OSCR, the Scottish Funding Council and the Financial Conduct Authority. They may also have regard to reports by non-governmental organisations and commercial due diligence providers.

Transaction Due Diligence

25. Due diligence is the process by which the University assures itself of the provenance of funds it receives and that it can be confident that it knows the people and organisations with whom it works. In this way the University is better able to identify and manage risk. Due diligence should be carried out before the funds are received. Funds must not be returned before due diligence has been reviewed.

26. In practical terms this means:

    i) identifying and verifying the identity of a payer or a payee, typically a student or a donor;

    ii) where the payment is to come from or to be made by a third party on behalf of the student or donor, identifying and verifying the identity of that third party;

    iii) identifying and verifying the source of funds from which any payment to the University will be made; and

    iv) identifying and in some circumstances verifying the source of wealth from which the funds are derived.

27. Source of funds refers to where the funds in question are received from. The most common example of a source of funds is a bank account. Source of wealth refers to how the person making the payment came to have the funds in question. An example of a source of wealth is savings from employment.

28. Guidance on how to do this when accepting payments from students will be provided through staff training.

Transaction Risk Assessment

29. Having completed its due diligence exercise, the University will assess the money laundering and terrorist finance risk associated with the proposed transaction.

30. Where the case falls into the category of case described as suspicious or the member of staff dealing with the case otherwise considers there is a suspicion of money laundering or terrorist finance, they must report the case as soon as practicable, by email, to the nominated officer at sarfinance@uws.ac.uk mailbox on a Form 1, which is to be found at Annex 1.

31. The Nominated Officer will consider the report and will decide:

    i) whether or not to accept or to make the proposed payment;

    ii) whether or not to make an authorised disclosure to the National Crime Agency; and

    iii) whether or not to make a disclosure under the Terrorism Act 2000.

32. The Nominated Officer will record in writing the reasons for their decision and retain that record centrally. Information that an authorised disclosure has been made must never be kept on the file relating to the person concerned.

33. Risk assessments relating to individuals and authorised disclosures are to be kept strictly confidential and should not be discussed within the finance department except on a strict need-to-know basis. No member of staff may reveal to any person outside the finance department, including specifically the student or third party funder in question, that an authorised disclosure or a disclosure under the Terrorism Act 2000 has been made.

Monitoring

34. The Nominated Officer will devise and implement arrangements to ensure that compliance with this Procedure is kept under continuous review through regular file reviews, including reviews of due diligence and risk assessment, and reports and feedback from staff. Internal audit may be called upon to assist in monitoring effective implementation of this Procedure.

35. To enable monitoring to be conducted and compliance with this Procedure to be evidenced, the University will retain all anti-money laundering and counter-terrorist

finance records securely for a period of at least five years.

Training

36. On joining the University any staff whose duties will include undertaking a finance function will receive anti-money laundering training as part of their induction process.

37. All staff undertaking a finance function will receive annual refresher anti-money laundering and counter-terrorist finance training.

38. The University's anti-money laundering and counter-terrorist financing training will include the applicable law, the operation of this Procedure and the circumstances in which suspicions might arise.

39. The University will make and retain for at least five years records of its anti-money laundering training.

Annex 1 – Student Due Diligence and Risk Assessment Form

Where finance staff know or suspect that fraud or money laundering has taken place they will not allocate the payment against the customer account but book the payment against GL code 4307 for further investigation. They will then answer the questions below and email this to the Suspicious Activity Reports sarfinance@uws.ac.uk mailbox as soon as practically possible.

1. **General details:**

Student or customer reference:

Payment / incident date:

Campus:

Select whether the main subject is a person or a legal entity:

2. **If subject is a person:**

Surname: Enter the subject's surname

Forename: Enter the subject's forename

Other names: Enter any other name(s) that the subject is also known as.

Title: Enter the title of the subject

Date of birth as 'dd-mm-yyyy' (if not known, leave blank).

Gender: Select the subject's gender, e.g. male.

Occupation: Enter the subject's occupation

Address: Enter the subject's address

3. **If subject a legal entity:**

Subject status: Select whether the entity in question is a suspect, victim or unknown.

Legal entity name: Enter the entity's name.

Legal entity number: Enter the entity's registered number – UK Enterprises registered under Companies House will have a unique registration number (if not known, leave blank).

VAT number: Enter the entity's VAT number (if not known, leave blank).

Business type: Enter the main type of business the entity engages in, e.g. solicitors.

Country of registration:

Address: Enter the business address

4. Transaction (this section can be skipped if there is no transactions to report relating to this disclosure)

If you have access to transaction history and transaction details, you can enter all details in this step.

Date: Enter the date of the transaction.

Amount: Enter the amount of the transaction.

Currency: Select from the drop down menu which currency the transaction is in, e.g. GBP (Pound Sterling).

Type: Select the type of transaction it is, e.g. cash, bank transfer.

Notes: Add any additional notes that you might have, e.g. if the payment was for accountancy services.

Account holder: Name of the account holder (this would be in the name of the main subject).

Account number: Main subject's bank account number.

Institution name: Name of the banking institution, e.g. Big Bank PLC.

Sort code: Banking institution's sort code (if not known, leave blank).

Date opened: Date the account was opened.

Date closed: Date the account was closed (if still active, leave blank).

Account balance: Amount of capital left in the account.

Balance date: Date of when the balance was taken.

Turnover credit: If you have knowledge of this please enter as appropriate.

Turnover debit: If you have knowledge of this please enter as appropriate.

Turnover period: Period during which these transactions happened (relates to 'i' and 'j').

5. Reason for suspicion/knowledge?

Provide as much detail as possible on why you are submitting this report, outlining the suspected money laundering activity and how all subjects entered are involved.

Necessary Information to include above:

I. the information or other matter which gives the basis for your knowledge or suspicion;
II. a description of the property that you know, suspect or believe is criminal property;
III. a description of the prohibited act.