ANTI MONEY LAUNDERING POLICY

Purpose and Context

The University of Huddersfield is committed to the highest standards of probity in all its financial dealings. It will therefore ensure that it has proper, robust, financial controls in place to 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 policy sets out those obligations, the University's response and the procedures to be followed to ensure compliance.

Scope

This policy applies to all individuals, including senior managers, deans, directors, employees (whether permanent, fixed-term or temporary), consultants, contractors, trainees, seconded staff, casual workers and agency staff, volunteers, interns, agents, sponsors, or any other person associated with us or any of our subsidiaries or their employees, wherever located (and collectively referred to as workers in this policy) who are engaged in financial transactions on behalf of the University.

Certain functions under this policy are to be undertaken by a Nominated Officer. For this policy, the Nominated Officer is the Director of Finance and, in their absence the Deputy Director of Finance.

Any failures to adhere to this policy may be dealt with under the University's disciplinary or other policies as appropriate. Note that any such failures also expose the individual concerned to the risk of committing a money laundering offence.

This policy does not form part of any employee's contract of employment and the University may amend it at any time.

---

1. What is money laundering?

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:

- **Placement** – the process of getting criminal money into the financial system
- **Layering** – the process of moving money within the financial system through layers of transactions; and
- **Integration** – the process whereby the money is finally integrated into the economy, perhaps in the form of a payment for a legitimate service.

2. Money Laundering Warning Signs or Red Flags

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

- Large cash payments.
- Multiple small cash payments to meet a single payment obligation.
- Payments or prospective payments from third parties, particularly where:
    - there is no logical connection between the third party and the student, or
    - where the third party is not otherwise known to the University, or
    - where a debt to the University is settled by various third parties making a string of small payments.
- Payments from third parties who are foreign public officials or who are politically exposed persons ("PEP").
- Payments made in an unusual or complex way.
- Unsolicited offers of short-term loans of large amounts, repayable by cheque or bank transfer, prepaid in a different currency and typically on the basis that the University is allowed to retain interest or otherwise retain a small sum.
- Donations which are conditional; on particular individual or organisations, who are unfamiliar to the University, being engaged to carry out work.
- Requests for refunds of advance payments, particularly where the University is asked to make the refund payments to someone other than the original payer.
- A series of small payments made from various credit cards with no apparent connection to the student and sometimes followed by chargeback demands.
- The prospective payer wants to pay up-front a larger sum than is required or otherwise wants to make payments in advance of them being due.
- Prospective payers are obstructive, evasive or secretive when asked about their identity or the source of their funds or wealth.
- Prospective payments from a potentially risky source or a high-risk jurisdiction.
- The payer's ability to finance the payments required is not immediately apparent or the funding arrangements are otherwise unusual.

3. Money Laundering - The Law

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

- The principal money laundering offences under the Proceeds of Crime Act 2002;
- The prejudicing investigations offence under the Proceeds of Crime Act 2002; and
- 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.

3.1 The Principal Money Laundering Offences

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 (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:

- Conceal, disguise, convert or transfer criminal property or to remove it from the United Kingdom.

- Enter into an arrangement that you know, or suspect makes it easier for another person to acquire, retain, use or control criminal property; and
- Acquire, use or possess criminal property provided that adequate consideration (i.e. proper market price) is not given for its acquisition, use or possession.

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.

3.2 Defences

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

Failure to Disclose Offence

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 practical after they received the information.

The Offence of Prejudicing Investigations /Tipping-Off

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 office if they tell a person an authorised disclosure has been made in their case.

Authorised disclosures must be kept strictly confidential.

4. Terrorist Finance

4.1 The Principal Terrorist Finance Offences

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.

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.

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

- Raising, possessing or using funds for terrorist purposes.
- Becoming involved in an arrangement to make funds available for the purposes of terrorism; and
- Facilitating the laundering of terrorist money (by concealment, removal, transfer or in any other way).

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

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.

Section 19 Terrorism Act 2000 creates an offence, punishable by up to five years imprisonment, 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 the report the matter either directly to the policy or otherwise in accordance with their employer's procedures.

4.2 The Offence of Prejudicing Investigations

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.

Disclosures made under the Terrorism Act 2000 must be kept strictly confidential.

5. Procedures

5.1 Overview

The University will:

- Conduct an annual risk assessment to identify and assess areas of risk money laundering and terrorist financing particular to the University.
- Implement controls proportionate to the risk identified.
- Establish and maintain policies and procedures to conduct due diligence on funds received.
- Review policies and procedures annually and carry out on-going monitoring of compliance with them.
- Appoint a nominated officer to be responsible for reporting any suspicious transaction to the National Crime Agency.
- Provide training to all relevant members of staff, including temporary staff, on joining the University, and provide refresher training, and
- Maintain and retain full records of work done pursuant to this policy.

The University's Risk Assessment, Continuous Review and Accountability

At least once a year, and more frequently if there is a major change in circumstances, the Director of Finance will:

- Conduct an assessment of money laundering and terrorist finance risk in the University's work
- Review and, if necessary, revise this policy in light of that risk assessment.

- Review and, if necessary, revise the University's arrangement for ensuring compliance with this policy so that resources are targeted to the areas of greatest risk; and
- Report to the Audit Committee on all aspects of this policy including its implementation.
- In order to facilitate the review and accountability functions the Director of Finance will ensure:
    - The availability of appropriate management information to permit effective oversight and challenge; and
    - The maintenance and retention of full record of work done under this policy.

In conducting the assessment of money laundering and terrorist financing risk arising from the University's work and funding activity, the Director of Finance will have regard to the University's experiences and to any lessons learned in applying this policy. They will also consider any guidance or assessments made by the UK government, law enforcement and regulators, including the Charity Commission, the Office for Students and the Financial Conduct Authority. They may also have regard to report by non-governmental organisations and commercial due diligence providers.

5.2 Transaction Due Diligence

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.

In practical terms this means:

- Identifying and verifying the identity of a payer or a payee, typically a student or a donor.
- 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.
- Identifying and verifying the source of fund from which any payment to the University will be made; and
- Identifying and in some circumstances verifying the source of wealth from which the funds are derived.

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.

5.3 Transaction Risk Assessment

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

Where a transaction is considered as suspicious, or the member of staff dealing with the transaction considers there is a suspicion of money laundering or terrorist finance, they must report the case as soon as practicable, by email to the Director of Finance based on the template in Appendix One.

6. Implementation

The Director of Finance is directly responsible to the Audit & Risk Committee for the implementation of this policy. As such, with the Committee's full support, they will ensure:

- Regular assessments of the University's money laundering and terrorist finance risks are conducted and relied on to ensure the effectiveness of this policy.
- Appropriate due diligence is conducted as a result of which risks relating to individual transactions are assessed, mitigated and kept under review.
- Anti-money laundering and counter-terrorist finance training is delivered within the University, including training on this policy and
- This policy is kept under review and updated as and when necessary, as levels of compliance are monitored.

7. Monitoring

The Director of Finance will devise and implement arrangements to ensure that compliance with this policy is kept under review through regular file reviews, including reviews of due diligence and risk assessment, and reports and feedback from staff.

To enable monitoring to be conducted and compliance with the policy 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.

8. Training

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.

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

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

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

Appendix One

Template email to send to the Director of Finance (copy and paste into the email)

SUBJECT: CONFIDENTIAL - Suspected Money Laundering

Your Name:	
School /Service	
Contact Details:	
Line Manager	
Details of the transaction:	
Name(s) and addresses of person(s) involved, together with details of their relationship with the university:	
Nature, value and timing of activity involved:	
Provide details of any investigation taken to date:	
Have you discussed your suspicions with anyone and if so: on what basis?	
Any other relevant information?	

POLICY SIGN-OFF AND OWNERSHIP DETAILS	
Document name:	Anti Money Laundering
Version Number:	V3.1
Equality Impact Assessment:	Previously considered – January 2022.
Privacy Impact Assessment:	PIA not applicable
Approved by:	Audit & Risk Committee on the recommendation of the University Senior Leadership Team.
Date Approved:	13 March 2025
Date for Review:	13 March 2028
Consulted with (Departments / Area of Service / Job Title):	Financial Services
Author:	Director of Finance
Owner (if different from above):	Director of Finance
Document Location:	Anti-Money-Laundering-Policy.pdf
Compliance Measures:	Audit, monitor of use of policy.
Related Policies/Procedures:	Financial Regulations Anti-Corruption, Bribery and Fraud Policy Donations Policy and Procedure

REVISION HISTORY

Version	Date	Revision description /summary of changes	Author
V3.1	January 2025	Minor revisions	Director of Finance
V3.0	January 2022	Major redraft (approval required)	Director of Finance
V2.1	February 2018	Minor revisions	Director of Finance
V2.0	June 2016	Minor revisions	Director of Finance
V1.0	July 2011	The first draft of a new policy	Director of Finance