Anti-Money Laundering Policy

Status	**Final**
Final Approval (UET)	**12 May 2026**
Final Approval (F&GPC)	**N/A**
Final Approval (ARC)	**N/A**
Court Approval	**N/A**
Publication on website	**Yes – May 2026**

Last Reviewed: **April 2026**

Next Review Date: **April 2027**

Contents

1. **Introduction**
2. **What is money laundering?**
3. **University responsibilities**
4. **Employee responsibilities**
5. **Know your customer**
6. **Record keeping requirements**
7. **Identifying money laundering: activities to be considered in relation to the University**
8. **Controls to mitigate the risk of money laundering**
9. **Disclosure procedure - how to report a concern**
10. **What the University will do - The Money Laundering Nominated Officer ("MLNO")**
11. **Staff Training**
12. **Appendix 1 Suspected Money Laundering Reporting Form**
13. **Appendix 2 MLNO Report**

1. Introduction

This Policy outlines how Glasgow Caledonian University, its UK subsidiary companies and any associated individuals will manage money laundering risks and comply with its legal obligations in accordance with the Proceeds of Crime Act 2002 and the Terrorism Act 2000. These Acts have detailed provisions which mean that they may cover activities carried on by persons inside and outside the United Kingdom. It is therefore important that those people acting for the UK based entities are aware of the Policy and abide by it when carrying on activities in the UK and other jurisdictions. This Policy applies to Court, Executive, Management, all staff, students, applicants, agents, volunteers, and to third parties, including academic partners, undertaking business on behalf of the University and its subsidiaries.

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

Reviewed on an annual basis, within the Policy Review Framework, this Policy will also be reviewed in line with the changes to relevant legislation. The Policy is available on the University website.

The requirements of the UK anti-money laundering regime are set out in:

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

The Money Laundering Regulations 2017 is the main piece of legislation in the UK which seeks to set procedures and standards to address and prevent money laundering. It is important to note that these regulations are not of universal application, applying only to organisations that are classified as 'relevant persons'. The University does not carry out any activities falling within the definition of 'relevant persons' thus falls out with the scope of these Regulations.

The Proceeds of Crime Act 2002 and Terrorism Act 2000 are not limited in their application and apply to all transactions; cheques, cash, bank transfers, property and equipment from individuals, agents or third parties.

The Counter Terrorism Act 2008 should not have direct effect on the University. This Act applies to persons operating in the financial sector; therefore, the University falls out with the scope of the provisions of this Act.

The Anti-Money Laundering Policy is one policy in a suite of counter fraud policies in place at the University, including:

- Financial Regulations (contact Finance)
- Financial Misconduct (contact Finance)
- Delegated Authority Policy (contact Finance)
- Criminal Facilitation of Tax Evasion Statement (contact Finance)
- Public Interest Disclosure Policy (contact People Services)
- Anti-Bribery Policy (contact Governance)
- Gifts & Hospitality (contact Governance)

2. What is money laundering?

Money laundering covers a wide variety of offences involving the proceeds of crime or terrorist funds.

It is the process by which criminally obtained properties are exchanged for 'clean' money or other assets with no obvious links to their criminal origins. Criminal property may take any form, including money or money's worth, securities, tangible property, and intangible property. For criminal property to exist there must be an element of criminal activity, which is defined as activity that constitutes an offence in the UK or would be if it occurred there.

Money laundering also covers money which is used to fund terrorism.

Money laundering schemes come with varying levels of sophistication from the very simple to the highly complex and can be carried out in any part of the world. 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. There are three stages in money laundering:

1) Placement – the process of getting criminal money into the financial system;
2) Layering – the process of moving the money within the financial system through layers of transactions; and
3) Integration – the process whereby the money is finally integrated into the economy. In the form of payment for a legitimate service.

Proceeds of Crime Act 2002 (POCA 2002)
This statue imposes various obligations on persons if they know about, and participate in, the laundering of the proceeds of criminal activity. Within the definition of this statute there are three principal offences and two third party offences that apply to the University.

Under the three principal offences, any person commits an offence, which is punishable by up to fourteen years imprisonment, if they:

- **Conceal, disguise, convert, or transfer** criminal property (Section 327 POCA 2002);
- Become concerned in an **arrangement** which they know, or suspect facilitates the acquisition, retention, use or control of criminal property (Section 328 POCA 2002);
- **Acquire**, **use** or have **possession** of criminal property (Section 329 POCA 2002).

A person commits a third-party offence if they:

- **Fail to disclose** if they know, or suspect, or have reasonable ground for knowing or suspecting money that another person is engaged in one of the three principal offences but fails to disclose this to the relevant officer or National Crime Agency (as applicable).
- **Tip off,** by informing a person(s) who are, or are suspected of being, involved in money laundering, in such a way as to reduce the likelihood of them being investigated, or prejudicing an investigation.

Terrorism Act 2000
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. 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 suspicion of terrorist finance for a number of different reasons, but typically might involve a request for payment, possibly disguised as a repayment or re-imbursement, to be made to an account in a jurisdiction with links to terrorism.

Similar to the Proceeds of Crime Act 2002, the Terrorism Act 2000 (section 15 to 18) creates offenses, punishable by up to fourteen years imprisonment, of:

1) raising, possessing or using funds for terrorist purposes;
2) becoming involved in an arrangement to make funds available for the purposes of terrorism; and
3) 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 cause to suspect that the funds concerned will be used for a terrorist purpose.

3. University responsibilities

Whilst much of the University's financial activities could be considered relatively low risk from the prospective of money laundering, all staff need to be vigilant against the financial crime and fraud risks that the University faces. Instances of suspected money laundering are likely to be rare at the University; however, we must be aware of the legislative requirements.

In order to manage the University's risk of money laundering, it has a responsibility to:

- Appoint a Money Laundering Nominated Officer (MLNO) to receive, consider and report as appropriate, disclosure of suspicious activity reported by employees;
- Implement a procedure to enable the reporting of suspicious activity;
- Maintain customer identification procedures ("know your customer (KYC)");
- Maintain adequate records of transactions;
- Publish and communicate this Policy to all employees.

4. Employee responsibilities

Money laundering legislation applies to **ALL** employees and members of Court. Potentially any member of staff could be committing an offence under the money laundering laws if they suspect money laundering or if they become involved in some way and do nothing about it. If any individual suspects that money laundering activity is, or has, taken place or if any person becomes concerned about their involvement it must be disclosed as soon as possible to the MLNO.

Failure to do so may result in you being personally liable to prosecution. Guidance on how to raise any concerns is included in this document (Section 10).

5. 'Know your customer'

Customer due diligence (CDD) is the process by which the University assures itself of the source of funds it receives and that it can be confident that it knows the people and organisations with whom it works. The Regulations require that the University must be reasonably satisfied as to the identity of the customer (and others) that they are engaging in a business relationship.

The University due diligence process follows the principles of "Know Your Customer (KYC)", one of the fundamental principles of global anti-money laundering regulations. The due diligence process ensures the identity of a new customer must be established before a business or financial relationship can begin with either an organisation or a student.

Both customer and geographical risk factors need to be considered in deciding the level of due diligence to be undertaken. Simplified due diligence is appropriate where the University determines that the business relationship or transaction presents a low risk of money laundering or terrorist financing. Enhanced due diligence is mandated for any business relationship with a person established in a high-risk third country. The list of high-risk countries as determined by the UK can be found here – High Risk Third Countries.

The UK government publishes frequently updated guidance on financial sanctions targets, which includes a list of all targets. This list can be found here - Financial Sanctions Targets.

The list provides information to assist in deciding whether the University is dealing with someone who is subject to sanctions. **The University will look to ensure that it has no relationship with any individuals on this list.**

Controls are in place to undertake customer due diligence i.e. steps to identify the student, customer or other party dealing with the University. Satisfactory evidence of identity must be verified.

For students on Campus, verification checks prior to issuing a student ID card include:

- UK student – review of a Passport or UK photo ID
- EU student – review of a Passport or EU Identity card
- International students – review of a Passport or Visa

For distance learner:

- Correspondence will be with the student at their home address

For sponsors:

- Letters or documents providing name and relationship to student should be obtained 'Sponsor letter'
- Aim to meet sponsors if appropriate to verify validity of contact

For third parties:

- Obtain letter headed documents showing a registered office and VAT number
- Request a credit check to be carried out by Finance

6. Record keeping requirements

By keeping comprehensive records, the University will be able to demonstrate that we have complied with legislation and managed our money laundering risks. This is crucial if there is a subsequent investigation into a transaction. Departments must maintain records with the University's Records Management for at least six years or in line with the University Record Management Policy.

The types of records kept include:

- Student/ customer identification records
- Receipts
- Cheques/ Pay-in books
- Customer correspondence

7. Identifying money laundering: activities to be considered in relation to the University

It is not possible to give a definitive list of ways to spot money laundering or how to decide whether to make a report to the MLNO. The following are risk factors which may, either alone or collectively, suggest the possibility of money laundering activity:

- A student or company pays fees by cash direct to the University and fails to provide proper evidence to confirm their identity and address;
- A person or company doing business with the University lacks proper paperwork, e.g. invoices that exclude VAT, failure to quote a VAT number or invoices issued by a limited company that lack the company's registered office and number;
- A student pays fees for another student who is not present at the time, without permission from the absent student;
- A sponsor/third party not known to the University pays fees for students without a logical reason or explanation;
- Overpayments for no reason;
- Significant changes in the size, nature, frequency of transactions with a customer that is without reasonable explanation;
- Unusual or unexpected large payments are made into the University accounts;
- A person or company attempts to engage in circular transactions, where a payment to the University is followed by an attempt to obtain a refund from the University's accounts;
- Cancellation, reversal or request for refunds of earlier transactions, particularly if there is a request to return money to a different account or individual to the payer.

Please note these examples are not intended to be exhaustive but provide a general indication of the range of matters covered by this Policy.

8. Controls to mitigate the risk of money laundering

In order to minimise the potential for money laundering activities, the University will follow the following procedures.

- It is University Policy not to accept cash payments for accommodation and tuition fees, and where possible, to not accept cash payments for other goods and services, instead preferring electronic payment.
- A student should not be permitted to pay the fees of another student who is not present at the time;
- Refunds made in respect of either student or non-student income should only be made by the same method and to the same account as the original payment was made;
- In the event of payment by credit or debit card being rejected, the reason should be checked with the card provider prior to accepting an alternative card;
- Fees paid in advance for overseas students who have subsequently been refused a visa are only refundable providing appropriate documentary evidence is received. Refunds can only be made by the same method and to the same account as the original payment was made;
- Students must make arrangements to cover their own living expenses. If a sponsor or third party pays funds in excess of tuition fees for such purposes, the funds cannot be transferred to the student. It can only be repaid by the same method and to the same account as the original payment was made.

9. Disclosure procedure – how to report a concern

When you suspect or know that a money laundering activity is taking, or has taken place, or you become concerned that your involvement in a transaction may amount to a breach of regulations, you should:

- use the Suspected Money Laundering Report Form at the end of this policy to report the

concern, giving as much information as possible, in writing, and without delay;

- email the Form as soon as possible to the University's Money Laundering Nominated Officer (MLNO) (email address below), marking the email "Confidential";
- Once you have reported your suspicions to the MLNO you should not make any further inquiries nor discuss your suspicions further unless instructed by the MLNO to avoid making a disclosure which may prejudice a money laundering investigation. At no time and under no circumstances should you voice any suspicions to person(s) you suspect of money laundering. This is to avoid committing the offence of "tipping off" those who may be involved.

10. What the University will do - The Money Laundering Nominated Officer ("MLNO")

The MLNO's role is to be aware of any suspicious activity in the University that might be linked to money laundering or terrorist financing, and if necessary to report it. They're responsible for:

- Receiving reports of suspicious activity from any employee in the University;
- Considering all reports and evaluating whether there is, or seems to be, any evidence of money laundering or terrorist financing;
- Report all reports received, whether potential or actual cases of money laundering to the Audit Committee;
- Reporting any suspicious activity or transaction to the National Crime Agency (NCA) by completing and submitting a Suspicious Activity Report; and
- Asking the NCA for consent to continue with any transactions that they've reported, and making sure that no transactions are continued illegally.

The MLNO for GCU is the Chief Operating Officer & DVC. In the absence of the Chief Operating Officer & DVC, the Chief Financial Officer or in their absence the Financial Controller will act as the MLNO.

Upon receipt of a completed Suspected Money Laundering Report Form, the MLNO will complete the MLNO Report. If appropriate, the MLNO will refer the case to the National Crime Agency (NCA) who will undertake any necessary investigation.

The MLNO will keep a copy of all reported suspicious transactions together with additional back-up and reasons for final conclusions, whether reported to the NCA or not for a minimum of 2 years (5 years for all instances reported to the NCA).

The University has a zero-tolerance approach to money laundering and will follow disciplinary action against anyone who is found to have committed a money laundering offence, which could result in dismissal for members of staff.

11. Staff Training

The University subscribes to training available from the British Universities Finance Directors Group website (BUFDG) and encourages all staff to use this resource as much as possible. The anti-money laundering training module on BUFDG should be completed by all Finance staff due to the nature of their roles.

12 Suspected Money Laundering Form

CONFIDENTIAL - Suspected Money Laundering Reporting Form Please complete and send this by email to the MLNO using the details below	
From:	**School/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:	12. 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, which carries a maximum penalty of 5 years' imprisonment and/or an unlimited fine.	

13 MLNO Report

MLNO Report (to be completed by MLNO only)			
Date report received: / /	Date receipt of report acknowledged: / /		
Consideration of Disclosure: [Please continue on a separate sheet if necessary]			
Action plan:			
Outcome of consideration of Disclosure:			
Are there reasonable grounds for suspecting money laundering activity?			YES/NO
If there are reasonable grounds for suspicion, will a report be made to the NCA?			YES/NO
If yes, please record the date of report to NCA and complete the details below: Date of report: / / Details of liaison with the NCA regarding the report: Notice Period: …….. to …….. Moratorium Period: …….. to ……			
Is consent required from the NCA to any ongoing or imminent transactions that would otherwise be prohibited acts? If yes, please confirm full details below:			YES/NO
Date consent received from NCA:			/ /
Date consent given by you to employee:			/ /
If there are reasonable grounds to suspect money laundering, but you do not intend to report the matter to the NCA, please set out below the reason(s) for non-disclosure:			
Date consent given by you to employee for any prohibited act transactions to proceed:			/ /
Signed		Date:	/ /
THIS REPORT TO BE RETAINED FOR AT LEAST FIVE YEARS			