University of St Andrews

Anti-Money Laundering

Document type	**Policy**
Scope (applies to)	All staff
Applicability date	30/04/2025
Expiry date	30/04/2027
Approved date	07/04/2025
Approver	Deputy Director of Finance
Document owner	Head of Financial Reporting
School / unit	Finance
Document status	Published
Information classification	Public
Equality impact assessment	None
Key terms	Financial matters/Income and debt management
Purpose	To set out the procedure to be followed if money laundering is suspected and defines the responsibility of individual employees in the process.

Version number	Purpose / changes	Document status	Author of changes, role and School or unit	Date
2025.01	Annual Update	Published	Head of Financial Reporting	01/04/2025

- British Sign Language (BSL) users can contact us via the online BSL Video Relay Interpreting Service: https://contactscotland-bsl.org
- This document and forms associated with this document are available in an alternative format upon request.
- We encourage employees to access the Probation webpage to access FAQs regarding the probation process, and download the forms referred to in this policy.

Contents

1. Statement

1.1 The University and its subsidiary companies ("the University") are committed to the highest standards of ethical conduct and integrity in their business activities in the UK and overseas. 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 policy outlines how the University and its employees will manage money laundering risks and comply with its legal obligations.

1.2 The key elements of the UK anti-money laundering framework that apply to universities are listed in Appendix I.

1.3 This policy complements the Criminal Finances Act 2017 policy and statement approved by the Principals Office which sets out the steps the University has taken, and will take, in relation to preventing the facilitation of tax evasion.

1.4 Other relevant policies that should be read in conjunction with this one are:

1.4.1 Financial Regulations

1.4.2 Fraud response policy

1.4.3 Treasury management policy

1.4.4 Whistleblowing procedure

1.4.5 Income and cash handling policy

1.4.6 Gift acceptance policy

2. Purpose

2.1 This policy enables the University to comply with its legal obligations and 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.

2.2 The University has a zero tolerance approach to money laundering and serious action will be taken against anyone found to be involved in money laundering, including dismissal under the University's disciplinary procedure.

3. Scope / jurisdiction

3.1 This policy applies to all University staff and Governors and covers all University activities undertaken in the UK or overseas. 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.

3.2 This policy outlines the University's arrangements to comply with the five key requirements of the money laundering regulations which are:

3.2.1 All organisations must obtain satisfactory evidence of the identity of each customer with whom it deals with and/or has a business relationship;

3.2.2 This evidence of client identity must be retained for the duration of the client relationship and for a period of five years after it terminates or in line with the University Record Management Policy; details of transactions must be kept for the same period;

3.2.3 Any suspicious transaction, whether in connection with a new or existing client, must be reported immediately to the Money Laundering Reporting Officer (MLRO);

3.2.4 The MLRO must, if deemed appropriate, report suspicion of money laundering to the appropriate authorities; in the UK this is the National Crime Agency (NCA)

3.2.5 Appropriate training must be provided to all relevant members of staff who handle, or are responsible for handling, any transactions with the organisation's clients and counterparties to ensure that they are aware of the organisation's procedures which guard against money laundering and the legal requirements of the money laundering rules

4. What is Money Laundering?

4.1 Money laundering is the process of taking profits from crime ('dirty funds') and transforming ('sanitising') them into legitimate assets. This process conceals the true origin or ownership of the funds, and so 'cleans' them. It also covers money, however come by, which is used to fund terrorism (reverse money laundering).

4.2 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:

4.2.1 Placement – the process of getting criminal money into the financial system;

4.2.2 Layering – the process of moving the money within the financial system through layers of transactions; and

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

5. Principal Money Laundering Offences

5.1 Appendix I summarises the three main types of offences in the UK. The Principal Money Laundering 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.

5.2 It is a crime, punishable by up to fourteen years imprisonment, to:

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

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

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

5.3 University staff can commit these offences when handling or dealing with any payments to the University by way of criminal activity or from being the proceeds of criminal activity (there is no minimal value). If a member of staff makes or arranges to make a repayment, they risk committing the first two offences, and if they accept a payment, they risk committing the third offence.

5.4 In all three cases, there is a defence if there has been an authorised disclosure of the transaction either to the Money Laundering Reporting Officer ("MLRO") or to the National Crime Agency ("NCA") and the NCA does not refuse consent to it.

5.5 It is a crime, punishable by up to five years imprisonment, for a MLRO 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.

5.6 Section 12 of this policy sets out how such disclosures are to be made.

5.7 The purpose of making an authorised disclosure to the NCA 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. This policy requires all authorised disclosures to be kept strictly confidential.

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

6.1 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 ("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 policy to managing risk.

7. Terrorist Finance – The Principal Terrorist Finance Offences

7.1 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.

7.2 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.

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

7.3.1 raising, possessing or using funds for terrorist purposes;

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

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

7.4 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.

7.5 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.

7.6 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 policy sets out those procedures at section 14 below.

8. The Offence of Prejudicing Investigations

8.1 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. This policy requires disclosures to be kept strictly confidential.

9. University Responsibilities

9.1 The University adopts a risk-based approach towards anti-money laundering and conducting due diligence. 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, but we must be aware of legislative requirements.

9.2 MLR 2017 requires the University to undertake a risk assessment, and to demonstrate and document that it was carried-out and has been/will be kept up-to-date. There are four main risk areas to review and these are listed in Appendix II along with examples of money laundering warning signs or "red flags".

9.3 To manage the University's risk of money laundering the University has:

9.3.1 Ensured this policy is proportionate to the specific risks identified;

9.3.2 Implemented internal systems, policies, controls and procedures to address money laundering and terrorist financing risks identified through the risk assessment;

9.3.3 Identified external controls including the banks who monitor and prevent transactions with sanctioned regimes;

9.3.4 Agreed customer due diligence procedures for transacting with students, customers and third parties;

9.3.5 Appointed a Money Laundering Reporting Officer (MLRO) to receive, consider and report as appropriate, disclosure of suspicious activity reported by employees;

9.3.6 Implemented a procedure to enable the reporting of suspicious activity;

9.3.7 Maintained adequate records of transactions; and

9.3.8 Undertaken appropriate staff awareness and training.

10. Customer Due Diligence

10.1 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. Therefore, the University has policies and procedures for performing CDD, and the transaction monitoring arrangements on a risk-managed basis with systems and controls in place to mitigate any financial crime risks. As required by the MLR 2017, we can demonstrate and have documented the risk assessment which will be reviewed periodically.

10.2 Our customer due diligence follows the principles of Know Your Customer (KYC), one of the fundamental precepts of global anti-money laundering regulations. This due diligence process ensures the identity of a new customer must be established before a business or financial relationship can begin or proceed.

10.3 The three components of KYC are:

10.3.1 Ascertaining and verifying the identity of the customer/student and confirming this by obtaining documentary evidence that is independent and reliable. In order to satisfy the requirements, identity checks are interpreted as obtaining a copy of photo-identification (such as a passport) and proof of address (such as a recent utility bill).

10.3.2 Ascertaining and verifying (if appropriate) the identity of the beneficial owners of a business.

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

10.4 In addition to a check on customers, the University must also undertake due diligence on transactions including:

10.4.1 Identifying and verifying the identity of a payer or payee, typically a student or donor

10.4.2 Where the payment is to come from or be made by a third party on behalf of the student/customer, identifying and verifying the identity of that third party through letters or documents proving name, address and relationship to the student.

10.4.3 Where an organisation is not known to the University:

10.4.4 Look for letter-headed documents, and/or

10.4.5 Check web-sites, and/or

10.4.6 Request credit checks, and/or

10.4.7 Aim to meet or contact key sponsors as appropriate to verify validity of contact.

10.4.8 Identifying and verifying the source of funds (ie, where the funds in question are received from, for example a bank account) from which any payment to the University will be made; and

10.4.9 In some circumstances identifying and verifying the source of wealth (ie how the person that is making the payment came to have the funds in question, for example savings from employment) from which the funds are derived.

10.5 Both customer and geographical risk factors need to be considered in deciding the level of due diligence to be undertaken. Simplified customer due diligence is appropriate where the University determines that the business relationship or transaction presents a low risk of money laundering or terrorist financing, taking into account the risk assessment. Under the UK's Money Laundering Regulations, enhanced due diligence (EDD) 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.

10.6 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.

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

11. Other Actions Taken

11.1 In addition to CDD, in order to minimise the potential for money laundering activities the University has the following procedures.

11.2 Cash payments

11.2.1 It is best practice to avoid accepting large cash payments for reasons associated with security and the risks associated with money laundering. It is therefore the University's policy not to accept

cash payments for accommodation or tuition fees, and where possible, to not accept cash payments for any goods or services preferring electronic payment instead.

11.3 Requests for refunds

11.3.1 Precautions should also be taken in respect of refunds requested following a payment by credit card or bank transfer. In these cases, refunds must only be made by the same method to the same account. In the event of an attempted payment by credit or debit card being rejected, the reason should be checked prior to accepting an alternative card. If in any doubt about the identity of the person attempting to make a payment the transaction should not be accepted.

11.3.2 Fees paid in advance by overseas students who have subsequently been refused a visa are only refundable providing appropriate documentary evidence is available to demonstrate the circumstances. Refunds should only be made to the person making the original payment, other than in exceptional circumstances where this is not possible.

11.3.3 Students must make arrangements to cover their own living expenses. If a sponsor or third party pays funds to the University in excess of tuition fees for such purposes, the funds cannot be transferred to the student. The funds can only be returned to the same account as the original payment was made and by the same method, other than in exceptional circumstances where this is not possible.

12. The Money Laundering Reporting Officer (MLRO)

12.1 The role of the MLRO is to be aware of any suspicious activity in the University which might be linked to money laundering or terrorist financing, and if necessary, to report it. They are specifically responsible for:

12.1.1 Receiving reports of suspicious activity from any employee of the University and maintaining a register of all reports;

12.1.2 Considering all reports and evaluating whether there is, or seems to be, any evidence of money laundering or terrorist financing;

12.1.3 Reporting of all reports received, whether potential or actual cases of money laundering to the University Vice-Chancellor;

12.1.4 Reporting any suspicious activity or transaction(s) to the National Crime Agency (NCA) by completing and submitting a Suspicious Activity Report;

12.1.5 Asking the NCA for consent to continue with any transactions that they have reported and ensuring that no transactions are continued illegally.

12.2 The MLRO for the university is the Chief Financial Officer:

12.2.1 E-mail: findir@st-andrews.ac.uk,

12.3 In their absence, the Deputy Director of Finance will act as MLRO:

12.3.1 E-mail: findep@st-andrews.ac.uk,

13. Employee Obligations and Disclosure Procedure to be Followed by Individuals

13.1 General expectations of employees include:

13.1.1 Discharge of duties in accordance with contractual obligations and with due regard to University policies and procedures;

13.1.2 Avoiding handling money, goods or other items known or suspected to be associated with the proceeds of crime, or becoming involved with any services known or suspected to be associated with the proceeds of crime;

13.1.3 Remaining vigilant and reporting ay concerns related to suspected money laundering activity;

13.1.4 Fully cooperating with any investigations into reported concerns;

13.1.5 Maintaining confidentiality about any suspected or actual incidents involving the University

13.2 Where you know or suspect that 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 the regulations, you must disclose this immediately to your line manager.

13.3 If you feel unable to discuss this with your line manager then please follow the whistleblowing procedure.

13.4 If, in consultation with your line manager, reasonable suspicion is confirmed, a disclosure report must be made to the MLRO. This disclosure should be

made on the Proforma report attached at Appendix III, as soon as practicable, by email, and giving as much detail as possible.

13.5 Once you have reported your suspicions to the MLRO you must not make any further enquiries into the situation unless instructed to do so by the MLRO. At no time and under no circumstances should you voice any suspicions to the person(s) you suspect of money laundering to avoid the offence of “tipping off” those who may be involved.

13.6 Failure to disclose a suspicion of a case of money laundering is a serious offence and may result in disciplinary procedures being instigated, potentially leading to dismissal and/or prosecution of the individual concerned.

14. Action and Disclosure by the MLRO

14.1 On receipt of a disclosure report the MLRO will complete the response form, attached at Appendix IV. Consideration will be given to all relevant information, including:

14.1.1 reviewing other relevant transaction patterns and volumes, and the length of any business relationship involved;

14.1.2 reviewing the number of any one-off transactions, linked one-off transactions, and any identification evidence held;

14.2 The MLRO will advise the individual concerned when a response can be expected.

14.3 The MLRO will make other reasonable inquiries as appropriate in order to ensure that all available information is considered when deciding whether a report to the NCA is required. Inquiries will be made in such a way as to avoid any appearance of “tipping off” those involved.

14.4 If the MLRO suspects money laundering or terrorist financing they will normally suspend the transaction and make a Suspicious Activity Report (SAR) to the NCA in a timely manner. However, a judgment will be made regarding how safe and practical it is to suspend the transaction without “tipping off” the suspect. It may be necessary to make the report as soon as possible after the transaction is completed.

14.5 Where the MLRO concludes that there are no reasonable grounds to suspect money laundering then consent will be given for transactions to proceed and the disclosure report will be marked accordingly.

14.6 The MLRO will keep a separate Register of money laundering report forms and will update this Register with any relevant documents as back up for the

reasons for their decision, including a copy of any SARs made to NCA and other NCA correspondence.

14.7 Information that an authorised disclosure has been made should never be kept on the file relating to the person concerned.

15. Record Keeping Requirements

15.1 By keeping comprehensive records, the University will be able to show that we have complied with money laundering legislation and managed money laundering risk. This is crucial if there is a subsequent investigation into one of our staff, students, customers or a transaction. The University retains records for at least five years or in line with the University Record Management Policy after ceasing to transact with a customer including records of customer risk assessment, customer identity and verification and customer ongoing monitoring.

16. Staff Training

16.1 In line with the Regulations, all relevant members of staff will receive training on this policy and the wider aspects of Anti Money Laundering. This will include new members, where the training will first be completed as part of their induction. Record keeping is crucial to an effective training regime and a record (or computer-based equivalent) should be kept verifying they have been trained on Anti Money Laundering.

16.2 The frequency of training for relevant staff should be determined on a risk-based approach but the periodicity should not exceed two years, unless there are unforeseen circumstances like a pandemic or equivalent..

16.3 The University also subscribes to the training available from British Universities Finance Directors Group website (BUFDG) and encourages staff to use this resource as much as possible. The anti money laundering training module on BUFDG is mandatory for all Finance staff to undertake, due to the nature of the roles.

17. Appendix I – Legislation and offences

17.1 Anti-Money Laundering laws that regulate financial systems, link money laundering (the source of funds) with terrorism financing (the destination of funds). The key elements of the UK anti-money laundering framework that apply to universities include:

17.1.1 Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ("MLR 2017") that includes the requirements of the EU's Fourth Money Laundering Directive (4MLD)

17.1.2 Proceeds of Crime Act 2002 (as amended by the Crime and Courts Act 2013 and the Serious Crime Act 2015)

17.1.3 Terrorism Act 2000 (as amended by the Anti-terrorism, Crime and Security Act 2001, the Terrorism Act 2006 and the Terrorism Act 2000 and Proceeds of Crime Act 2002 (Amendment) Regulations 2007)

17.1.4 Counter-terrorism Act 2008, Schedule 7

17.1.5 HM Treasury Sanctions Notices and News Releases

17.1.6 Joint Money Laundering Steering Group (JMLSG) Guidance

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

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

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

17.2.3 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.

18. Appendix II – Risk Areas and Money Laundering Warnings Signs

Risk areas	
Jurisdiction Risk	Risks associated with transacting with certain locations and jurisdiction including, but not limited to, the University's countries of operation, the location of customers, suppliers and/or agents, and transactional sources/destinations.
Customer/3rd party Risk	Risks associated with the people and/or organisations that we undertake business with including customers/3rd parties, beneficial owners, agents, contractors, vendors and suppliers. Politically Exposed Persons (PEP's) and Sanctioned Parties are also considered within this risk. Most of the University's customers are resident in the UK or EEA countries however some will come from/study overseas in potentially higher risk locations. The University also partners with overseas organisations for teaching and research purposes.
Distribution Risk	Risks associated with how the University undertakes business, particularly off campus, including direct and indirect relationships (via an agent or 3rd party), face-to-face, online and over the phone
Product/Service Risk	Risks associated with our standard product and service offerings. Whilst many of the University's operations do not present an opportunity for money laundering, there are risks around acceptance and processing of refunds.

18.1 We assess risks relevant to our operations and put in place the processes and procedures that we deem necessary to mitigate these risks. We determine the appropriate level of due diligence by looking at the geographic and customer risk factors based on the EU Directive and set out in MLR2017, and analysing the University's potential exposure to money laundering (the source of funds) or terrorist financing (the destination of funds).

Money Laundering Warning Signs or Red Flags

18.2 Payments or prospective payments made to or asked of the University can generate a suspicion of money laundering for a number of different reasons. Whilst it is not possible to give a definitive list of ways to spot money laundering, the following are examples of risk factors which may alone or collectively suggest the possibility of money laundering activity:

18.2.1 large cash payments;

18.2.2 multiple small cash payments to meet a single payment obligation;

18.2.3 payments or prospective payments from third parties, particularly where

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

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

c. a debt to the university is settled by various third parties making a string of small payments;

18.2.4 payments from third parties who are foreign public officials or who are politically exposed persons ('PEP');

18.2.5 payments made in an unusual or complex way;

18.2.6 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;

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

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

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

18.2.10 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;

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

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

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

19. Appendix III - Suspected Money Laundering - Report to the MLRO

From: ……..

School/Department: ……..

Contact Details: Email: ……..

Phone: ……..

DETAILS OF SUSPECTED OFFENCE

- 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.
- Provide details of any investigation undertaken to date.
- Have you discussed you 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: ……..

20. Appendix IV - MLRO REPORT (to be completed by the MLRO)

Date Report Received: ……..

Date Receipt of report acknowledged: ……..

CONSIDERATION OF DISCLOSURE

- Further action required:
- Are there reasonable grounds for suspicion requiring a report be made to NCA?
- If YES, confirm date of report to NCA:
- Address: UKFIU, PO Box 8000, London, SE11 5EN
- Fax: 0207 238 8286.
- Online: https://www.ukciu.gov.uk/(sct3dnqovty1ocisb5hzfy45)/saronline.aspx
- Any further details?
- Is consent required from NCA to any on-going transactions?
- If YES, confirm details and instructions:
  Date consent received:
  Date consent given to staff:
- If NO, confirm reason for non-disclosure
  Date consent given to staff:

Signed: ……..

Date: ……..

PLEASE RETAIN FOR AT LEAST FIVE YEARS

21. Version control

Version number	Purpose or changes	Document status	Author of changes, role and School or unit	Date
2025.01	Annual Review and Accessibility Changes	In Draft	MJS32 – Head of Financial Reporting	01/04/2025