



**Royal College of Art**  
Postgraduate Art and Design

# Anti-Money Laundering Policy and Procedures

Summary Information		
Document Owner	Chief Financial Officer	
Document Status	Approved	
Document Version / Date	March 2025	
Approving Committee	Audit and Risk Committee	12/03/2025
Date of Next Review	March 2028 or following changes in UK legislation	
Related Guidelines and Procedures	Financial Regulations Public Interest Disclosure (Whistleblowing) Policy Counter Fraud Policy and Fraud Response Plan Anti-Bribery Policy	

**Contents**

1. Introduction .....3

2. What is money laundering? .....3

3. Money Laundering Offences .....4

4. College Obligations, Monitoring and Compliance .....5

5. Due Diligence .....5

6. ‘Know your customer’ .....5

7. Employee obligations .....7

8. The Money Laundering & Proceeds of Crime Nominated Officer  
(MLNO) .....8

9. Disclosure Procedure to be followed by Individuals .....8

10. Action and Disclosure by the MLNO (Money Laundering Nominated  
Officer) .....9

11. Record Keeping Requirements .....10

Appendix 1 - Risks .....11

Appendix 2 - Suspected Money Laundering – report to the MLNO.....13

Appendix 3 - MLNO Report (to be completed by the MLNO) Date report  
received: .....14

Further information can be obtained from on [anti-money laundering regulations](https://www.gov.uk/government/topics/anti-money-laundering) gov.uk

## **1. Introduction**

- 1.1** This policy aims to ensure that the College, its students, employees, contractors, Council members and other related parties, comply with the legislation and that the highest standards of due diligence are applied in relation to 'know your customer' principles.
- 1.2** This policy:
- Defines money laundering;
  - Lays out the offenses provided for in current legislation;
  - Outlines how the College manages money laundering risks and complies with its legal obligations;
  - Sets out the procedure to be followed if money laundering is suspected;
  - Defines the responsibility of individual employees in the process.
- 1.3** The Royal College of Art ('the College') has a strict policy towards money laundering and does not tolerate activities that may facilitate money laundering, corruption, fraud or dishonesty.
- 1.4** The penalties for these offences are severe and can mean up to 14 years imprisonment and/or an unlimited fine for the employees and executives responsible. In addition, there would be significant reputational damage for the College.
- 1.5** This policy applies to all staff of the College and its subsidiary companies. It extends to all financial transactions and activities conducted by or on behalf of the College in the UK or overseas.
- 1.6** Any breach of this policy will be a serious matter, may result in disciplinary action and could result in an employee becoming personally liable to criminal prosecution.

## **2. What is money laundering?**

- 2.1** Money laundering is the act of concealing the origin and ownership of the proceeds of crime and corruption by transforming these proceeds into legitimate assets. It turns 'dirty funds' generated through illicit activity and converts them into other apparently lawful assets. This process is sometimes called 'cleaning'. In addition, most anti-money laundering (AML) legislation link money laundering (the source of funds) with terrorism financing (the destination of funds).
- 2.2** Money laundering arrangements have varying degrees of sophistication. The simplest may involve cash payments or cash transfers whilst the most complex can involve transferring money through multiple bank accounts and/or across borders.

**2.3** There are three stages in money laundering: placement, layering and integration.

- Placement – when the proceeds of crime enter the financial system;
- Layering – the process of distancing the proceeds from its original criminal source through layers of financial transactions;
- Integration – when the criminal proceeds are used in some way, appearing to be from a legitimate source.

**2.4** The approach to money laundering the College is required to take, is based on a framework of UK legislation and Financial Conduct Authority (FCA) rules.

**2.5** The following is a list of the elements of that framework:

- Proceeds of Crime Act 2002 (amended)
- Terrorism Act 2000 (as amended by the Anti-terrorism, Crime and Security Act 2001)
- Money Laundering, Terrorist Financing and Transfer of Funds (information on the Payer) Regulations 2017 (MLR 2017)
- Counter-terrorism Act 2008, schedule 7
- HM Treasury Sanctions Notices and News Releases
- Joint Money Laundering Steering Group (JMLSG) Guidance
- Sanctions and Anti-Money Laundering Act 2018

### **3. Money Laundering Offences**

**3.1** The penalties for breaching money laundering legislation are severe. The College could face a range of sanctions for non-compliance. Individuals connected to money laundering can face, depending on the type of involvement, unlimited fines and extensive prison terms.

**3.2** Any member of staff could be committing an offence under money laundering legislation if they suspect money laundering or if they become involved in some and do nothing about it. Staff who do not report suspicious activity in line with this policy may face disciplinary action and may be personally liable to prosecution.

**3.3** It is not possible to list all of the possible offences connected to the legislation but the following is a sample:

- Failing to report knowledge or suspicion of money laundering;
- Failing to have adequate procedures to guard against money laundering;
- Knowingly assisting money launderers;
- Tipping off suspected money launderers (Making a disclosure to a person which is likely to prejudice a money laundering investigation);
- Direct involvement in a money laundering scheme.

## 4. College Obligations, Monitoring and Compliance

### 4.1 The College has a responsibility to:

- Appoint a Money Laundering & Proceeds of Crime Nominated Officer (MLNO) to receive, consider and report as appropriate the disclosure of any suspicious activity reported by employees;
- Implement and maintain a procedure to enable the reporting of suspicious activity;
- Maintain customer identification procedures to 'know your customer' in relevant circumstances;
- Maintain adequate records of transactions.

### 4.2 The College is required to have appropriate systems and internal control mechanisms in place to mitigate the risk of money laundering. The College assesses risks relevant to its operations, and puts in place the processes and procedures that are necessary to mitigate these risks. Appendix 1 provides a list of typical risks associated with money laundering and the College's method for managing those risks.

### 4.3 Although instances of suspected money laundering are likely to be rare, given the nature of services provided by the College, failure to comply with legal requirements could have significant implications for both the College and individuals concerned.

## 5. Due Diligence

### 5.1 The College must assure itself of the origin of the funds it receives and be confident it knows the people and organisations with whom it works. Through due diligence the College is better able to identify and manage the risks that doing business represent. Due diligence should be carried out before funds are received. **Funds must not be returned before due diligence has been reviewed.**

### 5.2 In practical terms this means:

- Verifying the identity of a payer, customer or donor;
- Knowing where the payment is to come from or in cases of payments made by a third party on behalf of the student or donor, identifying and verifying the identity of that third party;
- Verifying the source of funds from which any payment to the College will be made.

### 5.3 The College determines the appropriate level of due diligence by looking at the geographic and customer risk factors as defined in the relevant regulations and legislation.

## 6. 'Know your customer'

**6.1** The College must be reasonably satisfied as to the identity of a student, other customer or third party and satisfactory evidence of identity must be obtained and retained.

**6.2** Our customer due diligence follows the principles of Know Your Customer (KYC). The three components of KYC are:

- Ascertaining and verifying the identity of the customer/student i.e. knowing who they are and confirming that their identity is valid by obtaining documents or other information from sources which are independent and reliable. In order to satisfy the requirements, identity checks for money laundering purposes are interpreted as obtaining a copy of photo-identification (such as a passport) and proof of address (such as a recent utility bill).
- Ascertaining and verifying (if appropriate) the identity of the beneficial owners of a business, if there are any, so that you the identity of the ultimate owners or controllers of the business is known.
- Information on the purpose and intended nature of the business relationship i.e. knowing what you are going to do with/for them and why.

**6.3** In the case of students this would include checking:

- Passport and/or Visa
- Birth Certificate
- Letters or documents proving name, address and relationship
- Checking against UK, US and EU sanctions lists

**6.4** For organisations not known to the College the following evidence can be helpful:

- Letter headed documents
- Invoices that show a company's registered office and VAT number
- Checking on limited company authenticity with Companies House
- A credit check
- Checking against UK, US and EU sanctions lists
- Meeting key contacts or sponsors to verify the validity of the contact

**6.5** Third party sponsors (eg donors or funders) should follow the same process as the one overseen by Advancement and Alumni for new donors.

## **6.6 Financial Sanctions Targets**

The UK Government publishes frequently updated guidance on financial sanctions targets, which includes a list of all targets. This guidance can be found at <https://www.gov.uk/government/publications/the-uk-sanctions-list>. The list provides information to assist in deciding whether the College is dealing with someone who is subject to sanctions. The Transaction Team review this list to ensure the College has no

relationship with any individuals on this list.

## **7. Employee obligations**

- 7.1** As mention in section 3 money laundering legislation applies to all College employees. 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.
- 7.2** If any employee 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. It is an offence under the current legislation to fail to report knowledge of money laundering activity. Guidance on how to raise any concerns is included in this policy document.
- 7.3** All staff must undertake mandatory training on Anti-Money Laundering, and must pass the related assessment. The training is available through the Staff Learning (sic) section of the [RCA Moodle](#).
- 7.4** The threshold for reporting suspicious transactions to the National Crime Agency is £1,000. This could include multiple smaller transactions that collectively exceed that limit.
- 7.5** The College does not accept payments in cash or cheque.

## **8. The Money Laundering & Proceeds of Crime Nominated Officer (MLNO)**

**8.1** The designated MLNO for the College is the Chief Operating Officer (<https://www.rca.ac.uk/more/organisation/governance/executive-board/>) in the absence of the MLNO the Chief Financial Officer is authorised to act as Deputy.

**8.2** The MLNO is responsible for the following:

- To receive and consider suspicious activity reports (SARs) and keep a register of the reports received;
- Inform the President and Vice Chancellor of all SARs received;
- Consider each report received and determine whether there is, or seems to be, any evidence of money laundering or terrorist financing;
- Report any suspicious activity or transaction(s) to the NCA by completing a SAR.
- Request a Defense Against Money Laundering (DAML) where appropriate;
- The MLNO will retain any disclosure reports and any associated relevant documents in a confidential file for a minimum of five years.

## **9. Disclosure Procedure to be followed by Individuals**

**9.1** Employees that suspect money laundering activity is taking or has taken place or are concerned that their involvement in a transaction may amount to a breach of the regulations must disclose this immediately to their line manager. If in consultation with the line manager reasonable suspicion is confirmed a disclosure report must be made to the MLNO.

**9.2** This disclosure should be made on the pro forma report attached at **Appendix 2** and should be completed the same day the information came to the employee's attention.

Employees that do not disclose in line with this policy may be personally liable to prosecution under the regulations.

**9.3** The report should include as much detail as possible including:

- Full available details of the people, including the people reporting, companies involved and other members of staff if relevant;
- Full details of transaction and nature of each person's involvement in the transaction;
- Suspected type of money laundering activity or use of proceeds of crime with exact reasons why you are suspicious;
- The dates of any transactions, where they were undertaken, how they were undertaken and the likely amount of money or assets involved;



- Any other information that may help the MLNO judge the case for knowledge or suspicion of money laundering and to facilitate any report to the National Crime Agency (NCA).

**9.4** Once reported to the MLNO employees must follow any instructions provided. Employees must not make any further enquiries unless instructed to do so by the MLNO.

**9.5** At no time and under no circumstances should the employee voice any suspicions to the person(s) suspected of money laundering nor should the matter be discussed with any colleagues. Failure in this regard could amount to tipping off and may constitute committing a criminal offence.

**9.6** If appropriate the MLNO will refer the case to the NCA who will undertake any necessary investigation. This may include consent to continue with a particular transaction and care should be taken not to 'tip off' the individuals concerned, otherwise the individual may be committing a criminal offence.

## **10. Action and Disclosure by the MLNO (Money Laundering Nominated Officer)**

**10.1** On receipt of a disclosure report the MLNO will:

- Note the date of the receipt and acknowledge receipt of it;
- Where appropriate, assess and advise the individuals concerned when a response can be expected;
- Consider the report and any other relevant information, undertaking further enquiries necessary to decide if a report should be made to the NCA;
- Inform the President and Vice-Chancellor.

**10.2** Once the MLNO has evaluated the case a timely determination will be made as to if:

- There is actual or suspected money laundering taking place
- There are reasonable grounds to know or suspect that is the case
- Consent is required from NCA for a particular transaction to proceed

**10.3** Where the MLNO concludes that the case should be disclosed to the NCA this needs to be done:

- In a timely manner;
- In the prescribed manner on a standard format report provided by NCA.

**10.4** Where the MLNO concludes that there are no reasonable grounds to suspect money laundering then consent will be given for transactions to proceed and the disclosure report proforma **Appendix 2** will be marked accordingly.

## **11. Record Keeping Requirements**

**11.1**By keeping comprehensive records the College will be able to show that it has complied with the Money Laundering Regulations. This is crucial if there is a subsequent investigation into one of our customers/students or transaction.

**11.2**The types of record kept may include:

- Daily records of transactions (ERP and associated payment platforms)
- Receipts
- Customer correspondence
- Student identification evidence

**11.3**Records may be kept in any of the following formats:

- Originals
- Photocopies
- Scanned
- Computerised/electronic

**11.4**The College's retention policy for financial records is 7 years. That is sufficient for money laundering purposes.

## Appendix 1 - Risks

Potential risk	Response
Large cash payments, or multiple small cash payments to meet a single payment obligation.	Cash payments are not accepted. Any attempt to pay in cash is refused and the payer is asked to use an alternative payment method.
Unusual or large payments are made into the College bank accounts from a potentially risky source or a high-risk jurisdiction.	<p>The College will make every effort to establish what the payment is for.</p> <p>The College bankers also advise on high-risk countries where financial transactions are either prohibited or heavily restricted and will not accept transactions from sanctioned banks or jurisdictions.</p> <p>The College does not advertise its bank details or provide them to unknown sources by telephone or email to limit the chances of unknown payments being received.</p>
A series of small payments made from various credit cards with no apparent connection to the student and sometimes followed by chargeback demands.	<p>Only transfers from students via one of the approved payment methods will be accepted. This currently limited to Flywire for student fees, Paypal for sundry payments and iZettle for shop and technical services payments.</p> <p>All online payments are made via a secure third-party. These third-party platforms do not accept payments from sanctioned countries or individuals.</p>
Donations which are conditional on individuals or organisations, who are unfamiliar to the College, being engaged to carry out work.	The due diligence is detailed in the College's <a href="#">Donations Acceptance Policy</a> .
A prospective payer who wants to pay up-front a larger sum than is required or otherwise wants to make payment in advance of them being due.	The College does not accept advance payments for sums greater than is required.
Prospective payers who are obstructive, evasive, or secretive when asked about their identity or the source of their funds.	Payers are required to follow the College's due diligence processes.
The payer's ability to finance the payments required is not immediately apparent or the funding arrangements are otherwise unusual.	Any payment plans which are not in line with College policy are approved by the Accounts Receivable Team. Payment proposals which appear suspicious in terms of affordability or source of funding are not accepted.
A person or company undertaking business with the College failing to provide proper paperwork (examples include charging VAT but failing to quote a VAT number or invoices purporting to come from a limited company, but lacking company registered office and number.)	The supplier approval process includes a credit check and a check of details at Companies House (if applicable). Suppliers that fail this will not be approved. Suppliers that fail to state information such as company or VAT registration number (where applicable) will be contacted by the Accounts Payable team who will investigate the supplier further prior to allowing the supplier to conduct business with the College.

<p>A potential supplier who submits a very low quotation or tender. In such cases, the business may be subsidised by the proceeds of crime with the aim of seeking payment from the College in “clean money.”</p>	<p>The College does not have to accept the lowest, or any, tender. Where a very low tender is received the Head of Procurement will undertake checks to ascertain why. This information is documented as part of the tender process.</p>
<p>Requests for refunds of advance payments, particularly where the College is asked to make the refund payment to someone other than the original payer.</p>	<p>Refunds will only be made back to source, and to the original payer. The Accounts Receivable team will undertake appropriate checks before any refund is processed to verify the identity of the person, reason and that it has been properly authorised.</p>

**Appendix 2 - Suspected Money Laundering – report to the MLNO**

**Contact details:**.....

**From:**.....

**School/ Dept.**.....

**Email**.....

**Phone**.....

**Details of suspected offence:**

- Name (s) and address(es) of person(s) involved including the relationship with the College
- Nature, value and timing of activity
- Provide details of any investigation undertaken to date
- Have you discussed your suspicions with anyone and if so on what basis
- Is there any aspect of the transaction(s) outstanding and requiring consent to progress
- Any other relevant information that may be useful

**Signed:**

**Date:**

**Appendix 3 - MLNO Report (to be completed by the MLNO) Date report received:**

**Date of receipt of report acknowledged:**

**Consideration of disclosure**

**Further action required**

Are there any reasonable grounds for suspicion requiring a report to be made to the National Crime Agency (NCA)

If YES: confirm date of report to NCA

**Link to NCA SAR online reporting system:**

<https://sarsreporting.nationalcrimeagency.gov.uk>

**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

**Signed:**

**Date:**