RCN Group Anti-Money Laundering Policy

Committees, Groups, Meetings to which this policy applies: RCN Group staff, members at all levels and members of Council, boards, external advisers and committees at any level.
Purpose of Document: Support and guidance for RCN Group staff and RCN members elected to office within the governance structure
Document Name: RCN Group Anti-Money Laundering Policy
Author/Authors: RCN Governance and Finance Teams; input from Bates Wells LLP
Description of Policy Guidance for RCN Group staff and RCN elected members on what money laundering is, how to recognise indications of it and report concerns instances of them, and the principles underpinning good practice, risk mitigation and due diligence.
Other policies, guidelines, legal positions etc that should be considered in conjunction with this policy: Whistleblowing Policy Conflicts of Interest Policy Gifts and Hospitality Policy Anti Bribery, Corruption and Fraud Policy Due Diligence Policy RCN Code of Conduct Regulation: RCN Council, board and committee members – fit and proper persons criteria Member resolution policy Staff Disciplinary Policy Group Risk Policy Statement of Investment Principles.
Circulated to: Executive Team (Oct 2022) Governance Support Committee (Nov 2022) Group Audit Committee (April 2023) RCN Foundation Board (July 2023) RCNi Board (July 2023)
Policy approved by RCN Council 27 July 2023
Date of implementation: July 2023
Date of next review: July 2026
Department responsible for Review: Governance team with input from FInance

POLICY SUMMARY: RCN GROUP ANTI-MONEY LAUNDERING

As a member of staff or elected RCN member you should:	As an organisation we will:
• Familiarise yourself with this policy and follow it. • Refer to any guidance or legal positions as referenced in the policy. • Understand RCN Group's zero-tolerance approach to money laundering. • Understand where money laundering may be indicated, and the process for reporting your concerns. • Follow the good practices of due diligence and risk mitigation outlined in the policy.	• Ensure that this policy and supporting information and processes are clear and accessible, and help elected members understand what they need to do. • Identify a team or individual responsible for keeping this policy under review and in line with any relevant updated guidance. • Provide advice, training and support on RCN Group's zero-tolerance approach to money laundering, recognising indications of it and how to report suspicions. • Review and/or audit this policy and associated processes and procedures every 2 years but mainly annually.

Royal College of Nursing

RCN Group Anti-Money Laundering Policy

1 Introduction

1.1 This policy sets out the procedure to be followed if anyone within the RCN Group suspects money laundering is taking place, as part of RCN Group's compliance with the Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017 (as amended), and the Proceeds of Crime Act 2002, Part 7 – Money Laundering Offences and the Terrorism Act 2000 (as amended, including as amended by the Crime and Courts Act 2013 and the Serious Crime Act 2015). The National Crime Agency is a crime-fighting agency with national and international reach with responsibilities for investigating money laundering and terrorist financing.

1.2 RCN Group has a zero-tolerance policy towards money laundering, and is committed to the highest level of openness, integrity and accountability in all our practices. The penalties for money laundering offences are severe and can include up to 14 years imprisonment and/or an unlimited fine for the individuals responsible (see also 4.3 below). Instances of this crime occurring as part of our activities would lead to significant financial/reputational damage for RCN.

2 Scope

2.1 This is an RCN Group policy and applies to all staff (see 2.2 below for more detail), members at all levels and members of Council, boards and committees at any level.

2.2 'RCN staff' means all employees including permanent/ongoing, temporary, fixed-term, consultants, those on fixed term contracts, trainees, seconded staff, home workers, casual workers, agency staff, volunteers and interns. (The term *employees* will normally be used throughout this policy to collectively refer to these categories).

2.3 The policy also applies to RCN Group's interactions with agents, sponsors, donors, external advisors or any other persons associated with the RCN Group (including third parties) regardless of where they are located, within or outside the UK. Note that *third parties* refers to any individual or organisation RCN Group works with, or with whom we have a business relationship. This includes actual and potential suppliers, distributors, business contacts, agents, advisers, government and public bodies and any party classified as a customer who is making payments to the RCN

Group. Any formal arrangements RCN Group makes with third parties are subject to clear contractual terms, including compliance with minimum standards and procedures relating to the provisions of this and associated policies.

2.4 The policy applies to all RCN Group activities undertaken by or on behalf of the RCN Group regardless of location, inside or outside the UK.

2.5 Any breach of this policy will be a serious matter, may result in disciplinary action and could result in an employee or member becoming personally liable to criminal prosecution (see 1.2 above).

2.6 This policy does not form part of any contract of employment or other contract to provide services, and we may amend it at any time.

3. Associated documents

3.1 This policy is part of a suite of documents aimed at ensuring best practice in governance. The related documents are:

- Whistleblowing Policy
- Conflicts of Interest Policy
- Gifts and Hospitality Policy
- Anti Bribery, Corruption and Fraud Policy
- Due Diligence Policy
- RCN Code of Conduct
- Regulation: RCN Council, board and committee members – fit and proper persons criteria
- Member resolution policy
- Staff Disciplinary Policy

3.2 It also operates in conjunction with the Group Risk Policy and the Statement of Investment Principles, and Disciplinary Policy and Procedure.

4 Policy aim

4.1 The legislative requirements concerning anti-money laundering procedures are lengthy and complex. This policy enables the RCN Group to meet its legal requirements in a way that is appropriate to its level of risk. This policy sets out to:

- highlight the RCN Group's zero tolerance approach to money laundering

- raise awareness throughout the RCN Group of what money laundering is and promote good practice in preventing it across the RCN Group and community
- explain how to recognise that money laundering may be taking place, what action to take and how to prevent it happening
- articulate the RCN Group's responsibilities in observing and maintaining its commitment to anti-money laundering (AML) practices
- signal that the RCN Group has effective procedures in place that mitigate the risk of being implicated in money laundering activities
- minimise, through the above actions, the risk of the RCN Group being party to criminal activity and consequent financial/reputational damage

5 Definitions

5.1 Money laundering is defined in the Proceeds of Crime Act (2002) as:

> *The process by which the proceeds of crime are converted into assets which appear to have a legitimate origin, so that they can be retained permanently or recycled into further criminal enterprises*

This means illicit funds are processed or spent to create the appearance that they have come from a legal source. Although cash-based money laundering continues to be the principal method in the UK, stricter rules have made it more difficult for criminals to introduce illicit funds into the banking system. Criminals are consequently using more inventive methods to disguise the origins of their cash. All in the RCN Group community must be alert to practices and payments that may seem suspicious, including payments made to the RCN Group via bank transfer.

4.2 There are three stages involved in money laundering:

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

If the RCN Group were to be party to the passage of illicit funds it could occur at any of the above stages.

4.3 UK legislation outlines a number of money laundering offences including:

- Failing to report knowledge or suspicion of money laundering

- Failing to have adequate AML procedures
- Knowingly assisting money launderers, including tipping-off suspected money launderers
- Recklessly making a false or misleading statement in the context of money laundering.

The penalties for breaching money laundering legislation are severe. Individuals connected with any stage of money laundering could face unlimited fines and/or prison terms ranging from 6 months to 14 years, depending on the offence. There are also sanctions for businesses that fail to comply with their AML obligations , imposed by HM Revenue and Customs (HMRC) and/or the Financial Conduct Authority (FCA).

5 RCN Group's AML responsibilities & reporting process

5.1 AML regulations require the RCN Group to assess its operations and activities with regard to the potential exposure to money laundering. There are four main areas of risk that need to be considered:

- Product/service risks relating to products and services offered across the RCN Group, such as member services, digital resources, products and events/conferencing offered by RCNi, the RCN Shop, receipt of donations and grants provided by the RCN Foundation.

- Jurisdictional risks associated with geography, location and jurisdiction including, but not limited to, any RCN Group activities undertaken outside the UK and the location of customers (including our members), suppliers and agents.

- Customer/third party risks associated with the people and/or organisations with whom we undertake business. This could be members, customers, suppliers and any other party having a contractual relationship with the RCN Group.

- Distribution risks in the context of how we undertake business, including direct and indirect relationships (for example via an agent or third party), face-to face, digital/online, telephone.

5.2 The RCN Group must maintain internal systems and controls in order to monitor transactions and any other activity involved in the above areas. This is done by:

- maintaining a procedure to enable the reporting of suspicious activity
- assigning, as part of the procedure, the role of Money Laundering Reporting Officer (MLRO) – this is a member of staff to whom disclosure of suspicious activity can be made and who considers the disclosures and acts as appropriate

- maintaining due diligence such as customer identification procedures in line with 'know your customer' principles (see 6.3 to 6.9 below)
- maintaining clear, accurate records of transactions

5.3 As explained in 2.1 and 2.2 above, AML legislation applies to all RCN Group employees and members. Any person could be committing an offence under AML law if they suspect money laundering is taking place, or if they become involved in such activity in some way, and do nothing about it. If any employee or member suspects that money laundering activity is happening or has taken place, or if any person becomes concerned about their involvement, it must be disclosed as soon as possible to the MLRO (see 5.2 above). Failure to do so could result in that employee or member becoming personally liable to prosecution. Guidance on how to raise any concerns is included below – see 5.8 to 5.12.

Further detail on risk considerations and related factors such as due diligence is given in section 6 below.

Roles and responsibilities

5.4 The RCN Group Finance Director has specific responsibility for the AML policy and oversight of AML culture and process (see also 6.10 below).

5.5 The Money Laundering Reporting Officer (MLRO) is a nominated member of staff and is the primary contact for any further information and to whom any suspicious activity is initially reported.

5.6 The Group Audit Committee is responsible for reviewing and monitoring this policy.

5.7 As per 5.3 above, each employee and member has a responsibility to be alert to suspicions of money laundering activity, and to maintain the due diligence practices outlined in section 6 below where this falls within their duties. There are 3 legal obligations placed on all RCN Group employees and members:

a) not to assist by acquiring, concealing, disguising, retaining or using the proceeds of crime or money used to fund terrorism;

b) not to prejudice an investigation into money laundering;

c) not to contact anyone suspected of, and reported for possible money laundering, in such a way that would make them aware of the suspicion or report (i.e. an obligation not to 'tip them off').

When considering these obligations staff should remember that the law requires all cases of suspicion to be reported regardless of size.

The checklist at Annex A should be used as a guideline when considering whether a transaction is potentially suspicious.

Reporting procedure

5.8 If you know or suspect that money laundering is taking place or has occurred, or you become concerned that your involvement in a transaction may amount to a breach of the AML regulations, you must disclose this immediately to the MLRO. This disclosure should be made using the Suspicious Activity Report (SAR) form – see Annex B. You may also discuss the disclosure in person with the MLRO but in every case the SAR must be completed. Any discussion, and completion/submission of the SAR, must be done in strict confidence. If you are unsure whether to report something to the MLRO please err on the side of caution and discuss your concerns with the MLRO at the earliest opportunity.

5.9 Once you have reported your suspicions to the MLRO you must follow any instructions given to you. You must not make any further enquiries 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, nor should you discuss the matter with any colleagues or fellow members. Failure to comply with this could result in a personal liability under the AML regulations.

5.10 The completed SAR must include as much detail as possible for the MLRO to make an informed judgement on how to proceed. The MLRO will report any findings to the Group Finance Director who will then proceed as appropriate based on the evidence provided in the SAR and any additional information obtained by the MLRO. If appropriate the MLRO or the Group Finance Director will refer the case to the National Crime Agency (NCA) who will undertake any necessary investigation and advise on any further action. This may include consent to continue with a particular transaction; if so, you must not alert the individuals concerned, otherwise you may be committing a criminal offence. *The penalty for tipping-off or prejudicing an investigation is 5 years imprisonment and/or an unlimited fine.*

5.11 If the MLRO concludes that there are no reasonable grounds to suspect money laundering, consent will be given for the relevant transaction(s) to proceed and the SAR will be marked accordingly and retained (see 6.11 to 6.13 below).

5.12 There are clearly defined procedures for dealing with allegations against employees and members which may apply in cases of corruption allegations if investigation reveals a breach of this policy or related ones (see 2.6 above). Such a finding may lead to dismissal of an employee or removal from membership of a member at any level. Breach of this policy by an agent, supplier, contractor or consultant acting on the RCN Group's behalf will lead to immediate termination of their contract. In addition to

implementing internal procedures we will notify the police or other authorities as appropriate, as well as the NCA as per 5.10 above.

6 Risk mitigation and due diligence

Risk considerations

6.1 The RCN Group has a risk-based approach to AML and due diligence. Most of our financial activities are relatively low-risk in terms of potential money laundering, but all staff nevertheless need to be vigilant regarding the possibility of financial crime and fraud. Instances of suspected money laundering are likely to be rare but we must be aware of the relevant legislative requirements and relevant risk factors. Annex A includes a checklist to help you identify potential suspicious activity. The circumstances identified in this checklist are not exhaustive and RCN employees and members should not limit their suspicions to the matters identified in that checklist. By way of example, scenarios that are at higher-risk of money laundering are:

- Where payments received by the RCN Group are unusual or have come from an unexpected source
- Where a payment is received from a third party from an account in a different name
- Where a third party is asking the RCN Group to reverse a payment because a payment has been made in error, and/or asking for funds to be returned to a different account to the account it originated from
- Where there are other unusual circumstances surrounding a payment e.g. the identity of the payer is unknown, the payer is anxious to make the payment quickly, the payer wants to make the payment in a number of instalments without a clear justification.

6.2 The RCN Group assesses risks relevant to our operations in line with the RCN Group Risk Policy and implements the necessary mitigations. We determine the appropriate level of due diligence in context of geographic and customer risk factors as set out in the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (known as MLR2017), Regulation 18.

Third party due diligence

6.3 In all financial transactions the RCN Group must be reasonably satisfied regarding the identity of a customer/supplier or other third party (see 2.3 above). To achieve this, satisfactory evidence of identity must be obtained and retained. This is done via customer due diligence following the Know Your Customer (KYC) principles, which are a set of guidelines used in the financial industry requiring that identity, suitability and risks are determined in relation to other parties in business relationships.

6.4 There are three key components of KYC which must be followed as part of compliance with MLR2017. These are:

- Identify the customer/supplier; verify their identity using documents or other information from independent and reliable sources

- If the customer/supplier is an organisation or legal entity, take reasonable measures to understand its ownership and control structure. You may need to verify the identity of the ultimate owners or controllers of the business

- Assess, and where necessary obtain information on, the purpose and intended nature of the business relationship or transaction. What are you going to do with/for the other party, and why?

6.5 Types of information that would help to achieve the above would include (but are not necessarily limited to):

- A copy of the third party's governing document e.g. Articles of Association for a company
- Letters or documents proving name, address and relationship
- Letterheaded documents (although these alone may not be sufficient as fake letterheads can be easily created)
- Invoices that show a company's registered office and VAT number
- Checking on limited company authenticity with Companies House and/or checking registrations with other regulators
- Credit checks – to be carried out in line with the RCN Group's procedures for ascertaining the creditworthiness of potential customers
- For individuals: passport, visa, birth certificate, proof of home address. Checking the provided name and address against the electoral roll (where based in the UK).

6.6 To comply with HMRC regulations, records of due diligence processes must be retained for five years from, at latest, the date on which the contractual relationship ends or the relevant transaction is completed. Failure to do so may be treated as a criminal offence.

Simplified and enhanced due diligence

6.7 Simplified due diligence (SDD) is permitted where risk assessment determines that the business relationship or transaction presents a low risk of money laundering. Regulation 37(3) of the MLR 2017 sets out a list of factors to be considered in determining whether a situation poses a lower risk of money laundering and thus allows SDD measures to be applied (see 6.9).

6.8 Enhanced due diligence (EDD): Regulation 33(1) of the MLR2017 (see 6.9) sets out a list of circumstances in which EDD measures must be applied, which includes any transaction or business relationship involving a party established in a 'high risk third country', or any transaction or business relationship involving a 'politically exposed person' presenting a higher risk of money laundering. Regulation 33(6) of the MLR2017 sets out a list of factors that must be taken into account in assessing whether there is a higher risk of money laundering and terrorist financing and the extent of EDD measures that should be applied. These must include, as a minimum, examining the background and purpose of the transaction and increased monitoring of the business relationship.

6.9 The full MLR2017 regulations can be found at The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (legislation.gov.uk)

Sanctions

6.10 The Group Finance Director ensures compliance with sanctions regulations set by the UN Security Council and the UK government which prohibit transacting with specific countries, groups and regimes (what is specifically prohibited under each financial sanction depends on the relevant regulation). Guidance can be found at Financial sanctions targets: list of all asset freeze targets - GOV.UK (www.gov.uk)

Record keeping

6.11 Maintaining comprehensive records is vital for demonstrating that we are complying with AML legislation, and is particularly important should there be any investigation into any third-party transactions. The types of record kept may include:

- Daily records of transactions
- Receipts
- Invoices
- Cheques
- Paying-in books
- Customer correspondence
- Third-party identity verification, including individuals' personal identification
- Ongoing monitoring/verification
- Risk assessments
- Written records of phone calls/conversations

6.12 Records may be kept as originals, photocopies, scanned copies, or other digital formats. All stored items and copies must be readable and dates clearly stated. Storage locations must be clearly labelled/indexed, the contents organised as methodically as possible.

In addition to the retention guidance given in 6.6 above, the MLRO will retain any SARs and any associated documents in a confidential file for a minimum of five years.

6.13 Storage of all the above information must be maintained securely with passcode access, with permissions clearly stated. (Note that the information may also be required for other purposes such as tax compliance).

7 RCN Foundation

7.1 As a registered charity, the RCN Foundation (charity no. 1134606) is subject to additional regulation by the Charity Commission. Where there is unusual or suspicious activity within the charity, the RCN Foundation Trustees should consider whether it is necessary to report that incident as a serious incident[1] to the Charity Commission. The Charity Commission guidance reminds charity staff and trustees to be alert to unusual donor activity, such as a large, one-off donation or a series of smaller donations from an unfamiliar, unverified or anonymous source; donations may take forms other than money, for example shares or goods.

7.2 An area where particular caution is needed is in relation to anonymous donations. The Charity Commission guidance states that charities are able to accept anonymous donations[2], subject to putting in place adequate safeguards and looking out for suspicious circumstances. An anonymous donation of £25,000 or more should ordinarily be reported to the Charity Commission as a Serious Incident, but the guidance confirms that[3] this will not be necessary in every case e.g. where an anonymous donation is via a solicitor who is aware of the donor's identity.

7.3 Anonymous donations received via intermediary professional service firms[4] are analogous to the solicitor example in the Charity Commission guidance and carry less risk, as the intermediary will have likely carried out some degree of due diligence already. Where an anonymous donation is proposed via an intermediary, you should seek to either identify the donor or confirm that the intermediary has done so; and then record in full the relevant factors leading you to accept or refuse the donation.

---

[1] https://www.gov.uk/guidance/how-to-report-a-serious-incident-in-your-charity

[2] See paragraph 5.2: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/677252/Chapter2new.pdf

[3] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752170/RSI_guidance_what_to_do_if_something_goes_wrong_Examples_table_deciding_what_to_report.pdf

[4] Examples of professional service firms include law firms, accountancy firms, trust companies, wealth management firms, investment firms

8. Communication and training

This policy is published on the RCN public website and the RCN's staff intranet site. All employees are asked to familiarise themselves with this policy when starting their employment with the RCN Group. Employees with finance responsibility receive appropriate AML training as part of their induction. Each member of the relevant team(s) are required to sign a record to verify that they have read and understood this policy. Refresher training takes place at each revision of the policy.

ANNEX A

ANTI-MONEY LAUNDERING – POTENTIAL SUSPICIOUS ACTIVITY CHECKLIST

Use this checklist to consider if payments and transactions are potentially high-risk in relation to money-laundering activity. If the answer to any of the questions is 'yes' the transaction must be referred to the Money Laundering Reporting Officer (MLRO) via the Suspicious Activity Report (SAR) report form – see Annex B.

The checklist is not exhaustive – even if all answers are 'no' but there is still any doubt or suspicion about the activity you should still refer it to the MLRO.

	AREA OF POTENTIAL SUSPICIOUS ACTIVITY (POSSIBLE RED FLAGS)	ISSUES TO CONSIDER	Y/N
1	Transactions	Are payments to us unusual because of their size, frequency or the manner of payment? Is the payer unexpectedly or unusually making lots of small payments from several different accounts? Are the payments unexpectedly being paid from a different account?	
2	Bank accounts	Is the payment being made from an account that is not in the same name as the payer?	
3	Arrangements	Does the payment involve complex or apparently illogical arrangements that make it unclear who is making the payment? eg: • Is the payment coming from a variety of sources or payers? • Is the payer seemingly unconnected to the donor/expected payer or recipient?	

4	Third-party payments	If the payment is from an account that is not the expected payer's account is the connection between the third-party making the payment and the RCN Group/receiving dept unclear?	
5	Internet search	Are there any adverse media items about the payer suggesting an involvement in criminal activities?	
6	Erroneous payments	Are we being asked to reverse a payment made because it was made in error? Are we being asked to send a repayment to a person that is different to the original payer?	
7	Country of origin	Is the payer resident in or recently relocated from a high-risk country? *Check with the MLRO about high-risk countries.*	
8	Politically exposed person (PEP: an individual performing a publicly prominent function)	Is the payer a PEP? If so, is their business activity unusual given the public role they hold?	
9	Assets	Does it seem that a payer's assets are inconsistent with their known legitimate income?	
10	Payment method	Are the payments being offered as bearer's cheques or cash?	
11	Identity	Is the payer difficult to identify? Is the payment being proposed as an anonymous donation?	
12	Early or quick payments	Is the payer unusually anxious to make a payment, and unable/reluctant to justify why they need to make the payment quickly or early?	
13	False documents	Do any documents associated with the transaction/ID checks appear to be falsified?	
14	Requests/incentives	Have you or colleagues/fellow members involved been: • instructed at remove • asked to act outside of your usual remit/duties • offered an additional/unusually high fee or other inducement?	

ANNEX B

ANTI-MONEY LAUNDERING – SUSPICIOUS ACTIVITY REPORT FORM

To be completed if any 'yes' answers are given when using the checklist at Annex A above, or if there is a possibility of suspicious activity not covered by the checklist.

This form must be completed and submitted in confidence to the MLRO when any of the questions in the checklist

CONFIDENTIAL	
SUSPICIOUS ACTVITY REPORT *To be completed if answering 'yes' to any of the questions in the Anti-Money Laundering Checklist, or if there are indications of possible suspicious activity not covered by the checklist. The completed form must be submitted in confidence to the Money Laundering Reporting Officer.*	
YOUR DETAILS	
Name	
Department/Team	
Email/Phone	
DETAILS OF SUSPICIOUS ACTIVITY	
Names and contact details of person(s) involved and relationship to RCN Group	
Description of activity including date(s) and value of transaction(s)	
Nature of suspicions regarding the activity	

Details of any enquiries you may have undertaken to date	
Have you discussed your suspicions with anyone? If yes please provide details including dates	
Are any aspects of the transaction(s) outstanding and requiring approval to progress/complete?	
Have you completed the Anti-Money Laundering Checklist?	
Signature and date	
THE SECTIONS BELOW TO BE COMPLETED BY MLRO ONLY	
Date report received	
Date report acknowledged to sender	
CONSIDERATION OF DISCLOSURE	
Are there reasonable grounds to suspect money laundering activity?	
Action plan	
Does the matter need to be reported to the NCA?	
If 'yes' to the above give date report made to the NCA and how the report was made (include any reference numbers provided as a result of the report)	
If 'no' to the above please set out rationale for non-disclosure to the NCA	
Is consent required from the NCA to proceed with a potentially suspicious	

transaction? If YES please confirm full details	