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 –

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 201

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.

5.2 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.

5.3 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).

6

Roles and responsibilities

6.4 The RCN Group Chief Financial Officer has specific responsibility for the AML policy and oversight of AML culture and process (see also 7.10 below).

6.5 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.

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

6.7 As per 6.3 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 7 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

6.8 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.

6.9 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.

6.10 The completed SAR must include as much detail as possible for the MLRO to make an informed judgement

- 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.

7.2 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

7.3 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.

7.4 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?

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

-

- For individuals: passport, visa, birth certificate, proof of home address.

- 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

7.12 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 7.6 above, the MLRO will retain any SARs and any associated documents in a confidential file for a minimum of five years.

7.13 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).

8 RCN Foundation

8.1 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.

8.2 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

[1] https://www.gov.uk/guidance/how-to-remission

e.g. where an anonymous donation is via a solicitor who is aware of the donor's identity.

8.3 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.

9. 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 10(tor)5(s)-49e8(o)4( )-3(the)4d t0.00

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