



Anti-Money Laundering

Approved: Summer 2022
Date of Next Review: Summer 2024

Equality Impact Assessment - Policy Review

In reviewing this policy, we have tried to make a positive impact on equality by considering and reducing or removing inequalities and barriers which already existed. We have ensured that this policy does not impact negatively on the dimensions of equality.

1. Introduction

The purpose of this policy is to ensure that The Roseland Multi Academy Trust ('Trust') staff are aware of, and comply with, the requirements of UK anti-money laundering legislation. This policy also sets out what measures, over and above those strictly required by law, the Trust has put in place to mitigate the risk of money-laundering occurring in the course of its business.

The risk of the Trust being targeted by those engaged in money laundering is likely small, due to the nature of education and its specialist supply chain. That said, the Trust is committed to detecting and preventing any money laundering activities, and to ensuring that it does not become involved in any arrangements involving criminal or terrorist property.

In order to fulfil this commitment, the Trust has established procedures for assessing the risk of financial crime, for internal reporting of suspicious activities and for making suspicious activity reports (SARs) to the relevant agencies.

Where risk factors are identified, the Trust will ensure that the identities of parents/carers, or other persons or organisations making any substantial payment to the Trust, are satisfactorily verified. Verification may take place at the beginning of their relationship with the Trust and, where appropriate, also at later stages.

The Trust will ensure that its staff are aware of the law in this area and will provide training where appropriate.

2. Legal Requirements

The law relating to money laundering is mainly covered in the Proceeds of Crime Act 2002 and the Terrorism Act 2000 & 2006.

There are two specific offences under the Proceeds of Crime Act 2002 that Trust staff should keep in mind:

- A person (which includes both individuals, and entities such as the Trust) commits an offence if he/she enters into, or becomes concerned in, an arrangement which he/she knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by, or on behalf of, another person;
- A person commits an offence if he/she acquires, uses or has possession of criminal property.

Property received by the Trust is criminal property if:

- It constitutes a person's benefit from criminal conduct or it represents such a benefit (in whole or part, and whether directly or indirectly), and;
- A member of staff knows or suspects that it constitutes or represents such a benefit.

There is a similar money laundering offence under the Terrorism Act 2000, if a person enters into or becomes concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property.

3. Assessing Risk

The Trust takes a risk-based approach to preventing money laundering, and therefore starts from the premise that the people with whom it does business are not money launderers or terrorists.

However, its procedures enable it to highlight any instances where there may be a higher risk of criminal activity and to apply appropriate control measures. These procedures have been designed as a proportionate and cost-effective response to the Trust's assessment of the actual risk.

When assessing risk, the Trust will take a variety of factors into account. These may include one or more of the following:

- *Jurisdiction*
If a person is resident in a jurisdiction that is perceived to have a lower standard of anti-money laundering regulation or measures to prevent corruption. This can be checked by reference to various indices, including the Transparency International Corruption Perceptions Index.

- *Politically Exposed Person(s) (PEP)*
A politically exposed person (known in the anti-money laundering regulations as a PEP) may be more at risk of being involved in money laundering. A PEP is a person who has been entrusted with prominent public functions, or any immediate family member or close associate of such a person.
- *Secrecy*
If a person is unusually secretive, for example if he/she is reluctant to meet face to face in circumstances where that would be the norm.
- *Sanctioned or Proscribed Organisations*
Whether the person is subject to sanctions or designated as, or associated with, a proscribed organisation.

Where a higher than usual level of risk has been identified, the staff concerned **must** consider whether it is appropriate to look more closely at any transaction and/or to require a more rigorous checking of identity and of the source of funds. In such cases it may also be deemed appropriate to arrange for routine monitoring of transactions so that, for example, any change in the source of funds used to pay the Trust is flagged up immediately.

4. Identification and Verification

Before entering into any transaction with a person or organisation with whom the Trust has no previous transactions or experience, the Trust may have need to take reasonable steps to ascertain the identity of that person or organisation.

In the case of individuals, the key information is:

- Full name
- Residential address
- Date of birth

Depending on whether particular risk factors are present, the Trust may seek independent verification of identity, for example by requiring originals or certified copies of official documents confirming identity. Suitable documents might include passports or birth certificates.

When checking such documents, staff must be alert to any signs that they might have been forged or stolen. The Trust will consider the option of using commercial verification services, particularly in relation to overseas jurisdictions where the Trust may have limited access to the relevant databases and records.

In relation to organisations that are not already known to the Trust, staff will check websites, perform a company search and where appropriate they will request credit checks and/or aim to contact key personnel in the organisation.

Staff should also check whether third parties are designated as, or associated with, proscribed organisations by checking the person's name against the UK government's current sanctions and proscribed organisations list, available on the gov.uk website.

5. Reporting Suspicious Activity

The Trust is not required by law to have a Money Laundering & Proceeds of Crime Nominated Officer (MLNO) to whom suspicious transactions or activities should be reported but, as part of its commitment to detecting and preventing any money laundering activities, it has decided that the Chief Financial Officer (CFO) should act as the MLNO and, in his/her absence, the Chief Executive Officer (CEO) supported by the Trust Management Accountant(s).

The function of the MLNO is to:

- Act as a single point of contact for staff in relation to any suspicions of money laundering or other financial crime;
- Oversee the provision of training and guidance to staff;

- Provide reports to Trustees, if requested, on the operation and effectiveness of the Trusts' anti-money laundering procedures; and
- Keep this policy and related procedures under review.

As the MLNO, the CFO has additional obligations in respect of reporting suspicious activities to the National Crime Agency (NCA) and the Police ensuring that, where a report has been made, no steps are taken without the consent of the NCA or police where required.

Failure to comply with these obligations can be an offence under section 332 of the Proceeds of Crime Act.

6. Grounds for Suspicion

It is not possible to produce an exhaustive list of the matters that might give rise to a suspicion of money laundering or other financial crime. It is therefore important that staff are provided with training in the general issues and encouraged to use their own judgment when looking at any new business relationship or transaction.

The following are some of the possible warning signs:

- Unusually secretive behaviour, including reluctance to provide requested information without a reasonable explanation;
- Payment of any substantial sum in cash (over £1,000);
- Doubts about the honesty, integrity, identity or location of the people involved;
- Involvement of a third party without a logical reason or explanation;
- Any overpayments for no good reason;
- Any doubt as to the ability of a person to have a legitimate source of the funds received;
- Significant changes in the size, nature and frequency of transactions with a fee-payer or donor that is without reasonable explanation, for example if payments start to be made from a different jurisdiction;
- Cancellation, reversal or requests for refunds of earlier transactions;
- A history of poor business records, controls or inconsistent dealing;
- Requests for account details outside the normal course of business.

7. Disclosure Procedures

Staff must make a report to the MLNO where they have knowledge or suspicion, or where there are reasonable grounds for having knowledge or suspicion, that another person is engaged in money laundering, or that terrorist property exists.

Where concerns or suspicions relating to the MLNO exist, the same process should be followed, but must be reported directly to the CEO and Chair of Trustees.

Your report should include as much detail as possible including:

- Full available details of the people and/or organisations involved, including yourself 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 reasons for your suspicion;
- The dates of any transactions, where they were undertaken, how they were undertaken and the likely amount of money or assets involved;
- Information on any investigation undertaken to date, including whether the suspicions have been discussed with anyone and if so on what basis;
- Whether any aspect of the transaction(s) is outstanding and requires further action to progress; and
- Any other information that may help the MLNO judge the case for knowledge or suspicion of money laundering and to facilitate any external report.

It is the Trusts' policy, following a disclosure to the MLNO or to the NCA and the Police, not to do or say anything that might either prejudice an investigation or "tip off" another person that a disclosure has been made.

Once you have reported your suspicions to the MLNO you must follow any instructions provided. You must not make any further enquiries unless instructed to do so by the MLNO. Any further transactions or activity in respect of the person in question, whether or not it is related to the matter that gave rise to the original suspicion, should be reported to the MLNO as they happen, unless and until the MLNO has confirmed that no report to the NCA and the local police is to be made.

The MLNO must consider all internal reports and must make an external report to the NCA (who will undertake any necessary investigation) as soon as is practicable if he/she considers that there is knowledge, suspicion or reasonable grounds for knowledge or suspicion, that another person is engaged in money laundering, or that terrorist property exists. This applies even if no transaction takes place.

The MLNO will report any suspicions of money laundering activity, and how they have been managed, to the CEO and Board of Trustees.

8. Record Keeping

The Trust will retain copies of the evidence obtained of the identity of people and organisations with whom it has done business for five years after the end of the business relationship, together with details of all transactions.

All suspicions reported to the MLNO must be documented, either on paper or electronically. The report should include full details of the person or organisation that is the subject of concern and as full a statement as possible of the information giving rise to the knowledge or suspicion. All enquiries that are made within the Trust in relation to the report should also be recorded.

The Trust must also keep details of actions taken in respect of internal and external suspicion reports, including details of information considered by the MLNO in respect of an internal report where no external report is made.

9. Receiving Cash Payments

If any member of Trust staff is offered funds that he/she knows or suspects are criminal property or may represent terrorist finance, or if he/she receives any unusual request to receive or transfer money, it must be reported immediately to the MLNO who will, if appropriate, contact the NCA, Police or other relevant agency.

As part of a risk-based approach to the receipt of funds, all parents are encouraged to pay Trust fees through its online payment systems from a UK bank account. Staff should not accept payments in cash in excess of £1,000 in any circumstances and, any cash receipt in excess of £1,000 must be approved in advance by the MLNO.

Precautions must be taken in respect of refunds requested following a payment by credit card or bank transfer. In such cases, refunds should only be made by the same method to the same account, unless authorised by the MLNO.

10. Contacts

National Crime Agency: 0370 496 7622 (available 24/7)
<https://www.nationalcrimeagency.gov.uk/communication@nca.gov.uk>

NCA Headquarters
Units 1 - 6 Citadel Place,
Tinworth Street,
London
SE11 5EF