Special Partnership Trust

MONEY LAUNDERING POLICY

Date Last Reviewed: September 2021

Review Date: September 2022

Money Laundering Policy

Introduction

The Proceeds of Crime Act 2002, the Terrorism Act 2000 and the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 place legal obligations on the Trust and its employees - regarding suspected money laundering activity.

Although most money laundering activity in the UK falls outside of the public sector, we are committed to maintaining robust arrangements to identify and prevent attempts to use it to launder money. The vigilance of employees is vital in identifying individuals who are, or may be, perpetrating crimes relating to money laundering or the financing of terrorism.

Scope of the Policy

This Policy applies to all employees of the Trust. It aims to maintain the high standards of conduct which currently exist within the Trust by preventing criminal activity through money laundering. The Policy sets out the procedures which must be followed, for example the reporting of suspicions of money laundering activity, to enable the Trust and employees to comply with legal obligations.

This Policy sits alongside the Trust's Fraud Policy and Whistleblowing Policy.

Failure by an employee to comply with the procedures set out in this Policy may lead to disciplinary action being taken against them in accordance with the relevant Disciplinary Procedures.

Whilst the risk of contravening the legislation is low, it is extremely important that all employees are familiar with their legal responsibilities, as breaches of the legislation could result in criminal prosecution and upon conviction imprisonment for up to 14 years and/or a fine.

What is Money Laundering?

Money laundering is the term used for a number of offences involving the proceeds of crime or relating to the proceeds of terrorism and terrorist financing.

Money laundering is generally defined as the process by which the proceeds of crime, and the true ownership of those proceeds, are changed so that the proceeds appear to come

from a legitimate source. In effect it is the process of channelling “bad” money into perceived “good” money, to hide the fact that it originated from criminal activity.

The following constitute acts of money laundering:

- Concealing, disguising, converting, transferring criminal property or removing it from the UK (Section 327 of the Proceeds of Crime Act 2002)
- Entering into or becoming concerned in an arrangement that you know, or suspect facilitates the acquisition, retention, use or control of criminal property by, or on behalf of, another person (Section 328)
- Acquiring, using or possessing criminal property (Section 329)
- Becoming concerned in an arrangement facilitating concealment, removal from the jurisdiction, transfer to nominees or any other retention or control of terrorist property (Section 18 of the Terrorism Act 2000).

These are the primary money laundering offences and are prohibited acts under the legislation. There are also a number of secondary offences relating to the failure to report a person known, or suspected, to be engaged in money laundering or terrorist financing and the falsifying, concealing or destroying of documents relevant to an investigation or making a disclosure which is likely to prejudice it.

What is the impact on the Trust?

Potentially any employee could be caught by the money laundering provisions if they suspect money laundering or become involved with it in some way and do nothing about it. The officer nominated to receive disclosures about money laundering/terrorist financing activity within the Trust is the CEO.

If you know or suspect that money laundering activity is taking/has taken place, or you become concerned that your involvement in a matter may amount to a prohibited act under the legislation, you must disclose this as soon as practicable to the CEO.

The report should include as much information as possible, but you must not make any further enquiries into the matter yourself or continue with the transaction. You must follow any subsequent direction from the CEO who will guide and support you throughout the process.

At no time and under no circumstances should you voice any suspicions to the person suspected of money laundering, or to any other individual, whereby doing so you could prejudice an investigation. Likewise, you must not make any reference on a client file that a report has been made to the CEO, in case this results in the suspect becoming aware of the situation.

The CEO must promptly evaluate any disclosure report to determine whether it should be reported to the National Crime Agency (NCA) by submitting a Suspicious Activity Report (SAR). You will be informed if a SAR is made. If the CEO concludes that there are no

reasonable grounds to suspect money laundering, then this will be duly recorded, and they will give their consent for any ongoing or imminent transaction(s) to proceed. Ultimately it will be the responsibility of the CEO to decide whether there is a reasonable excuse for not reporting the matter to NCA.

If a SAR is made to NCA, "consent" that gives a defence from a principal offence can be requested from them to perform the transaction but the transaction in question must not be undertaken or completed until "consent" is given, or there is deemed "consent" through the expiry of relevant time limits.

In all cases where a SAR is made to NCA, the CEO will advise you if and when you can continue with a transaction.

All disclosure reports made to the CEO and reports referred to NCA must be retained for a minimum of five years.

Identification of Clients (Customer Due Diligence Procedure)

If the Trust is carrying out certain "relevant business" (accountancy, audit and tax services and legal services relating to financial, company or property transactions) and:

a) Forms an ongoing business relationship with a customer; or

b) Undertakes an occasional transaction amounting to £10,000 or more, whether carried out in a single operation or several linked ones; or

c) Suspects money laundering or terrorist financing; or

d) Doubts the veracity or adequacy of information previously obtained for the purposes of client identification or verification,

then care needs to be taken by the Trust to check the identity of the customer. This is known as carrying out Customer Due Diligence and must be applied before the establishment of the relationship, or the carrying out of the transaction.

Applying Customer Due Diligence means:

a) Identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from reliable and independent sources;

b) Assessing, and where appropriate obtaining, information on the purpose and intended nature of the business relationship; and

c) Where someone else purports to act on behalf of the customer, verifying their identity and that they are authorised to act for the customer.

Where the "relevant business" is being provided to another public sector body then you should ensure that signed written instructions on that body's headed paper, or an email from the body's e-communication system, is obtained before any business is undertaken.

Where the customer is a corporate body it is necessary to obtain and verify:

a) The name of the corporate body;

b) Its company number or other registration number;

c) The address of its registered office, and if different, its principal place of business; and take reasonable measures to determine and verify:

d) The law to which the body is subject, and its constitution (whether set out in its articles of association or other governing documents); and

e) The full names of the board of directors and the senior persons responsible for the operations.

Where the customer is beneficially owned by another person it is necessary to:

a) Identify the beneficial owner so that we are satisfied that we know who the beneficial owner is, including, in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangement; and

b) Take reasonable measures to verify the identity of the beneficial owner.

In some circumstances, enhanced due diligence must be carried out, for example:

- The case has been identified as one where there is a higher risk of money laundering or terrorist financing;
- The customer is a "politically exposed person" or a family member or close associate of such a person;
- The business relationship or transaction is with a person established in a high-risk third country (a high-risk state other than an EEA state)
- The transaction is complex and unusually large, or there is an unusual pattern of transactions and the transactions have no apparent economic or legal purpose.

Ongoing due diligence must be carried out by the relevant Trust during the life of a business relationship, but should be proportionate to the risk of money laundering or terrorist funding based on knowledge of the customer and regular scrutiny of the transactions involved.

If enhanced due diligence is required this must also include, as far as reasonably possible, an examination of the background and purpose of the transaction and increased monitoring of the business relationship to determine whether anything appears to be suspicious.

If the required due diligence measures have not been undertaken then the business relationship or one-off transaction(s) cannot proceed any further and any existing business relationship with that customer must be terminated.

Ongoing Monitoring and Record Keeping Procedures

Any Trust conducting "relevant business" must monitor, on an ongoing basis, their business relationships, scrutinising transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds), to ensure that the transactions are consistent with their knowledge of the client, its business and risk profile.

Records of all client identification/verification evidence obtained (or references to it) and details of all "relevant business" transactions carried out for customers, must be maintained for at least five years beginning from the date the specific business relationship ends. This is so that the records may be used as evidence in any subsequent investigation by the authorities into money laundering. At the end of the five-year period any personal data obtained must be deleted unless:

- It is required to be retained under any enactment or for the purposes of any court proceedings; or
- The data subject has given consent for the data to be retained; or
- There are reasonable grounds for believing the records need to be retained for legal proceedings.

The precise nature of the records is not prescribed by law. They must, however, be capable of providing an audit trail during any subsequent investigation, for example distinguishing the client and the relevant transaction and recording the source of, and in what form, any funds were received or paid.