



## Anti-Money Laundering Policy

The Foundation could be used as a vehicle through which criminals seek to launder the proceeds of crime (**Illicit Funds**). Additionally, the Foundation, or a member of staff, is at risk of committing a money laundering offence if they accept Illicit Funds in circumstances where they have knowledge or a reasonable suspicion that the payment is from Illicit Funds.

Members of staff need to be vigilant to the risk of accepting Illicit Funds and play their role in assisting law enforcement agencies in combatting money laundering. The Proceeds of Crime Act 2002 (**POCA**) (as amended from time to time) imposes obligations on the Foundation and you personally, in respect of money laundering and associated activities. The purpose of this policy is to:

- assist staff with identifying red flags that may be indicative of money laundering activities;
- reduce the risk of the Foundation being used as a vehicle through which criminals can launder Illicit Funds; and
- let staff know what they should do if they have a concern that the Foundation is at risk of accepting Illicit Funds.

Linked to this, there are charity law requirements to ensure that reasonable skill and care are used when making decisions about procedures for the receipt and use of the Foundation's funds.

### What is money laundering?

Money laundering is the process by which Illicit Funds are processed or spent to create the appearance that the Illicit Funds have come from a legal source. Although cash based money laundering continues to be a major method of laundering Illicit Funds in the UK, stricter rules have made it more difficult for criminals to introduce Illicit Funds into the UK banking system. Consequently, criminals are using more inventive methods to disguise the origins of their cash and staff should be alert to practices and payments that they consider to be suspicious, including payments made to the Foundation via bank transfer.

The term 'money laundering' covers several offences each of which relate to the improper handling of Illicit Funds so that they appear to come from a legitimate source. Money laundering underpins most forms of organised crime, allowing criminals to further their operations. However, it can also benefit individuals engaging in bribery and dishonest activities such as receiving stolen goods or tax evasion.

### Money Laundering is described as:

*"a scheme in which criminals try to disguise the identity, original ownership, and destination of money that they have obtained through criminal conduct. The laundering is done with the intention of making it seem that the proceeds have come from a legitimate source".*

### Risks to the Foundation

The Foundation is potentially vulnerable to being used as vehicle through which a criminal may seek to launder Illicit Funds, for example a criminal may use their Illicit Funds to pay fees or make a donation. Although fee payments are clearly an area of risk, as a member of staff you should remain alert to all payments and if a payment seems unusual, for example where it involves complex banking and transfer arrangements or



payments from seemingly unconnected third parties you should refer the payment to the Director of Finance and Resources.

Whilst the Foundation is unlikely to have satisfied the threshold for committing a money laundering offence where the Foundation or member of staff was unaware that a payment was made from Illicit Funds, as a member of staff you must not turn a blind eye. Where there are factors, 'red flags', that indicate a higher risk of potential money laundering activity, you must refer the concern to the Director of Finance and Resources who will consider what further steps or investigations are required before accepting the payment.

Even if the Foundation has not committed a money laundering offence, if criminals use Illicit Funds to make payments to the Foundation, being involved in an instance of money laundering may have a severe impact on the Foundation's reputation.

### **Cash payments**

Criminals are increasingly inventive in finding ways to introduce Illicit Funds into the banking systems and although payments made through a bank transfer cannot guarantee that the funds are not from Illicit Funds the risk to the Foundation is increased where the Foundation accepts payments in cash. Accordingly, it should be the exception that cash payments of more than £100 are accepted.

In exceptional cases the Foundation may allow a larger payment to be made in cash. Before agreeing to accept a large cash payment, the Director of Finance and Resources will consider the circumstances relating to the payment. The Director of Finance and Resources must obtain evidence to satisfy the Foundation that the payment is being made from a legitimate source. Such enquiries might include asking the parent for:

- an explanation of why the payment is being made in cash;
- information on how the cash was obtained; and
- proof of this.

The Director of Finance and Resources must consider the explanation and information provided by the parent and decide whether the Foundation is able to accept the cash payment. In each case, the Director of Finance and Resources will make and retain a record of the decision made and the supporting evidence. Where the parent is not able to provide a satisfactory explanation, the Foundation must not accept the cash payment.

If the Director of Finance and Resources is not satisfied that the funds are clean, the Director of Finance and Resources must consider whether, in the circumstances the Foundation should:

- make a suspicious activity report (**SAR**) to the National Crime Agency (**NCA**); and
- make a report to the Charity Commission.

### **Key areas of risk for the Foundation**

Money laundering can take many forms, but in relation to the Foundation it could involve, but will not be limited to:

- the payment of fees;
- the payment of fees from third parties;
- the donation of sums to projects for which an appeal is being run;
- the donation of sums for no obvious reason;
- the payment in advance of fees; and



- the requested return of donation or fees paid in advance.

These examples are not exhaustive, and as a member of staff you should remain vigilant in relation to all payments the Foundation receives.

### Donations

Donations are a particular area of potential risk faced by the Foundation. To mitigate the risk the Foundation should know, at least in broad terms, where the money it is being given comes from and should be able to identify and be assured of the provenance of substantial donations. A good, open and transparent relationship between the Foundation and its donors is essential for building trust and confidence.

Good due diligence will help to:

- assess any risks to the Foundation that may arise from accepting a donation or types of donations;
- ensure that it is appropriate for the Foundation to accept money from the particular donor;
- give the Foundation reasonable assurance that the donation is not from any illegal or inappropriate source; and
- ensure that any conditions that may be attached the donation are appropriate and can be accepted.

Where a donation is being made the relevant member of staff should review what they know about the donor and the proposed payment using the checklist in the Annex to this policy. The completed checklist must be provided to the Director of Finance and Resources who will keep a record of the findings.

If when, completing the checklist, the member of staff identifies any red-flags, the member of staff must report the concern to the Director of Finance and Resources immediately.

### Requests for repayments

The Foundation's policy is that any refunds or repayments of sums paid to the Foundation can only be remitted to the bank account that made the payment. If a parent or donor asks for a refund to be made to a different account, in particular one that belongs to someone other than the original payer, you must refer this to the Director of Finance and Resources promptly.

### Charity Commission

When accepting payments or donations the Foundation needs to be confident that it knows both:

- who is making the payment or donation; and
- the source of funds that are being used to fund the payment.

The Foundation will also use the following Charity Commission advice to assess the risk of money laundering:

- **'identify'** who the Foundation is dealing with;
- **'verify'** where reasonable, and if the risks are high, verify identities;
- **'know what the organisation's or individual's business is'** and be assured this is appropriate for the Foundation to be involved with;
- **'know what their specific business is with the Foundation'** and have confidence that they will deliver what we want them to; and



- **'watch out'** for unusual or suspicious activities, conducts or requests.

If the Foundation is not satisfied with the explanation or evidence provided to support these factors the Foundation should obtain further information from the parent or donor. The section below ***"What warning signs should staff be alert to?"*** provides an indication of the circumstances when the Foundation must carry out further investigations about the payer.

### **What warning signs should staff be alert to?**

The Annex to this policy provides members of staff with a non-exhaustive checklist of potential 'red flags' that may indicate a higher risk of potential money laundering. These questions form part of the Foundation's risk assessment when accepting payments. They are potentially relevant to all transactions and payments accepted by the Foundation.

The Foundation is not expected to consider every payment in detail against the red flag checklist and will consider payments on a risk basis. The Director of Finance and Resources has identified the payments listed below as being payments that may expose the Foundation to a higher risk of money laundering. If a proposed payment is within one of the specified risk categories, you must complete the 'red flag' checklist before the Foundation can accept the payment:

- donations
- cash payments over £100
- payments from high-risk countries
- payments from PEPs

The Director of Finance and Resources has identified countries that it considers to be high-risk countries and will review and update this list on a regular basis. You should ask the Director of Finance and Resources for the most recent list of countries when you are considering whether a payment is a potentially high-risk payment.

Where payments are within one of the risk categories listed above members of staff must consider the payment against the red flag checklist before the payment can be accepted by the Foundation. You must promptly report any concerns to the Director of Finance and Resources.

All staff, but particularly those staff who in the course of their day-to-day work are likely to deal with financial transactions, including the payments of fees and donations, must ensure that they are familiar with the checklist and understand the nature of the red flags that should be reported to the Director of Finance and Resources. If you identify a red flag in relation to any payment or proposed payment you must report your concerns to the Director of Finance and Resources immediately.

Where you make a report to the Director of Finance and Resources you ***must not discuss your concerns*** with any other person, including other members of staff, pupils, parents or a donor as this could result in you, or the Foundation, committing a secondary offence of prejudicing an investigation.

### **What must the Director of Finance and Resources do where a payment seems suspicious?**

Where a member of staff identifies a red flag in relation to a payment the Director of Finance and Resources must consider the relevant circumstances relating to the transaction that has raised the concern. The enquiries the Director of Finance and Resources will make will depend on the circumstances, but could include:



- asking the payer to explain who is making the payment where this is not clear;
- asking for an explanation of why the payment is being made in a particular way, for example, where payments are being made from a variety of sources or accounts;
- asking the payer for proof of the source of the funds; or
- carrying out a google or other internet search to establish that the payer is not involved in alleged criminal activities.

After having made appropriate enquiries, the Director of Finance and Resources will decide whether:

- the payment can be accepted;
- further explanation or evidence as the legitimacy of the funds is required;
- the Foundation should submit a SAR; and
- the Foundation should make a report to the Charity Commission.

The Director of Finance and Resources will keep a record of the decision made in relation to the payment and the evidence supporting the decision.

### Reporting to the National Crime Agency and Charity Commission

If the parent (or payer) or donor is not able to provide a satisfactory explanation or where there are other factors (for example adverse media publicity) that cause the Director of Finance and Resources to have a reasonable suspicion or knowledge that the funds being used to make the payment may be Illicit Funds the Director of Finance and Resources must make a suspicious activity report (**SAR**) to the NCA and, where appropriate request consent to proceed with the transaction.

If the Foundation has requested a defence against a money laundering offence (**DAML**) in the SAR the Foundation should not accept, pay away, return or otherwise use the suspicious payment for any purpose until the time limit for the NCA to respond to the SAR has expired.

The Director of Finance and Resources will also consider whether the incident needs to be reported also to the Charity Commission.

### Training

The Foundation will train its relevant staff from time to time on how to limit the money laundering risks faced by the Foundation, by enabling staff to spot potential 'red flags' and what steps they must take if a potential risk factor is identified.

If any member of staff has any concerns or would like further information on what they should do in the event of a concern about money laundering the member of staff should contact the Director of Finance and Resources in the first instance.

October 2021

## APPENDIX 2

### Checklist for Identifying Potentially Suspicious Transactions

You must consider the following questions in relation to each high-risk payment. If any of the answers to the questions are "yes", you must refer the payment to the Director of Finance and Resources for further consideration. This list is not exhaustive. Even if all the answers to the questions are "no" if something seems unusual you must raise your concern with the Director of Finance and Resources.

	Potential red-flags	Ask...	Yes/ No
1.	<b>Transactions</b>	Are payments to the Foundation unusual because of their size, frequency or the manner of their execution? For example: Is the parent unexpectedly or unusually making lots of small payments from several different accounts? Are the payments unexpectedly being paid from a different account?	
2.	<b>Bank account:</b>	Is the payment being made from an account that is not in the same name as the payer?	
3.	<b>Arrangements</b>	Does the payment involve complex or illogical arrangements that make it unclear who is making the payment? For example: Is the payment coming from a variety of sources or payers? Is the payer seemingly unconnected to the pupil, parent or donor?	
4.	<b>Third party payments</b>	If the payment is from an account that is not the parent's account is the connection between the third-party making the payment and the pupil unclear? For example, is the payment from someone who is not the parent's employer or a known relative of the pupil?	
5.	<b>Internet search</b>	Are there any adverse media articles about the payer suggesting an involvement in criminal activities?	
6.	<b>Erroneous payments</b>	Has the Foundation been asked to reverse a payment made because the payment was made in error? Has the Foundation been asked to send a repayment to a person that is different to the original payer?	
7.	<b>Country of residency</b>	Is the parent resident in or have they recently relocated from, a high-risk country? You should ask the Director of Finance and Resources for the current list of high risk countries.	



8.	<b>PEP (Politically Exposed Person – broadly an individual who is performing a prominent public function)</b>	Are either of the parents or the person paying the fees (where different) a PEP? If the parent is a PEP, is their business activity unusual given the public role they hold?	
9.	<b>Assets:</b>	Does it seem that a parent’s assets are inconsistent with their known legitimate income?	
10.	<b>Resources</b>	Are the funds being used bearer's cheques or cash?	
11.	<b>Identity</b>	Is the payer difficult to identify?	
12.	<b>Early or quick payments</b>	Is the parent unusually anxious to make a payment? Is the parent unable to justify why they need to make the payment quickly or early?	
13.	<b>False documents</b>	Do any documents appear to be falsified?	
14.	<b>Representative</b>	Have you, or other professionals involved been instructed at a distance, asked to act outside of your usual specialty, or offered an unusually high fee?	



## APPENDIX 3

### Firms Offering Technological Solutions to Assist with Minimising Money Laundering Risk

#### 1. Flywire

Flywire is a tuition fee payment processor and is used by more than 1,800 institutions worldwide and 60 independent Foundations in the UK.

The Flywire solution offers institutions a secure online payment portal to improve the way tuition fees and related payments from students and parents are collected. Through Flywire, institutions can limit the number of technical integrations required, have visibility over the payment life cycle, and reduce time spent on the reconciliation of payments whilst offering their payers multiple payment options, from credit card and bank transfer to e-wallet options.

This reduces the need or incentive for any payer to risk transporting large amounts of cash across borders for payment at the institution. Payers can be directed to make a payment through Flywire prior to arrival at the institution.

As a payment institution authorised by the Financial Conduct Authority, Flywire is subject to compliance with anti-money laundering and fraud rules and regulations. The company is required to ensure that it has an anti-money laundering compliance programme in place in order to reduce risk, and to include adequate controls to prevent financial crime against its business and clients.

When making refunds to payers, the Flywire solution includes the ability to limit the financial crime risks and fraud risks, offering a managed solution to ensure and verify that the funds are always returned to the originating source.

Flywire contact details: Flywire London, 45 Folgate Street, 4th Floor, London, E1 6GL

Email: [tom.jones@flywire.com](mailto:tom.jones@flywire.com)

[www.flywire.com](http://www.flywire.com)