

ANTI-MONEY LAUNDERING POLICY

Last reviewed:	April 2025
Next review due:	April 2026
Reviewed by:	Data Compliance Administrator

1. Definition

Money laundering is the process by which the proceeds of criminal or illegally obtained money are processed or spent to create the appearance that they have come from a legal source.

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”. (ISBA)

It is a term designed to cover several offences. These offences relate to the improper handling of funds that are the proceed of criminal acts or terrorist acts. It relates to both the activities of organised crime but also to those who benefit financially from dishonest activities such as receiving stolen goods.

The school is potentially vulnerable to this threat and the consequences of being involved in an instance of money laundering may have a severe impact on the school's reputation.

2. The school's responsibility

Money laundering can take many forms, but in relation to the school it could involve:

- payments made in cash;
- the payment of fees;
- the payment of fees by third parties;
- the payment in advance of fees;
- the requested return of fees paid in advance;
- the donation of sums to projects for which an appeal is being run; and/or
- the donation of sums for no obvious reason.

The school must be vigilant in relation to all payments, particularly where these involve complex banking and transfer arrangements. Where there are concerns, 'red flags', that indicate a higher risk of potential money laundering activity, you must refer the concern to the Director of Finance & Operations who will consider what further steps or investigations are required before accepting the payment.

These activities may also add to a second 'laundering' activity by which illicit wealth is used to bolster the reputation of a family by having their child or children in a prestigious independent school.

3. Cash payments

Cash payments should be rare, and cash payments of more than £100 should not be accepted. It may be, very exceptionally, that a cash donation, or the payment of a term's fees has to be accepted. If so, this would be classed as a large or unusual transaction and the school will ask the parent, guardian or benefactor for information on how the cash was obtained and seek proof of this.

If the payer is not able to provide a satisfactory explanation, the school must not accept the cash payment.

4. Requests for repayment

The school's policy is that any refunds or repayments of sums paid to the school 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, the member of staff must refer this to the Director of Finance & Operations immediately.

5. Donations

The school must know where the money it is being given comes from and be able to identify and be assured of the provenance of substantial donations. In addition, the donation must be for a legitimate appeal or purpose. A good, open and transparent relationship between the school and its donors is essential for building trust and confidence.

When 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 **Annex A** below. The completed checklist must be held by the Director of Finance & Operations as a record of the findings.

6. Risk assessment

The school will use the following Charity Commission advice to assess the risk of money laundering, because the principles are applicable despite the school not being a charity:

- **'identify'** – know who the school is dealing with;
- **'verify'**¹ – verify identities, where this is reasonable and if the risks are high;
- **'know what the organisation's or individual's business is'** – and be assured it is appropriate for the school to be involved with it;
- **'know what their specific business is with the school'** – and have confidence that they will deliver what the school wants them to; and
- **'watch out'** for unusual or suspicious activities, conducts or requests.

Red Flags include:

- donations
- cash payments over £100
- payments from high-risk countries
- payments from a Politically Exposed Person (PEP)

Bursary staff will consult the questions in **Annex A** as part of a risk assessment to assess the source of money being offered to the school.

If one or more of the factors in the risk assessment is present the school will make further enquiries to satisfy itself that the payment is being made from legitimate sources before the school accepts the payment. Concerns must be reported to the Director of Finance & Operations.

The risk assessment should also be completed for every sum of more than £100 accepted in cash.

In addition the school uses Flywire as the preferred payment means for collecting international income to reduce the risk. Further details are provided in **Annex B**.

7. Named people subject to financial sanction

To aid with sanction searches, the school will use the search tool issued by the UK Office of Financial Sanctions Implementation <https://sanctionssearch.ofac.treas.gov>.

The UK government and ICAEW have released the following lists of people world-wide who are subject to financial sanctions in the UK, including those sanctioned due to Russia's involvement in Ukraine: [Who is subject to financial sanctions in the UK?](#)

If the school discovers any of these names in connection with the school, their resources will be frozen and the matter reported to the Office of Financial Sanctions Implementation.

8. Admission sanctions

The school will follow admissions guidelines contained in the Nord Anglia Education document 'Guidance on Sanctions Monitoring – guidance to schools' Admissions and Finance teams' (available from the [NAE SharePoint](#)). The school will not engage in any transaction with any person or entity in countries subject to US and UK financial sanctions programmes.

Sanction checks will be based on the nationality of the parents and guardians, not that of the student.

9. Further action by the Director of Finance & Operations

Concerns reported to the Director of Finance & Operations must not be discussed with any other person, including other members of staff, students, parents or a donor as this could result in the member of staff, or the school, committing a secondary offence of prejudicing an investigation.

The Director of Finance & Operations will investigate any concerns regarding the legitimacy of a payment to decide whether the payment can be accepted.

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

10. Reporting to the National Crime Agency

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 & Operations to have reasonable suspicion or knowledge that the funds being used to make the payment may be Illicit Funds, the Director of Finance & Operations must make a Suspicious Activity Report (SAR) to the National Crime Agency and, where appropriate request consent to proceed with the transaction.

If the school has requested a Defence Against a Money Laundering offence (DAML) in the SAR the school should not accept, pay away, return or otherwise use the suspicious payment for any purpose until the time limit for the National Crime Agency to respond to the SAR has expired.

*

Associated policies:

School policies available from the [school website](#):

- Anti-bribery and corruption policy
- Anti-fraud policy

Nord Anglia Education policies available to staff from the [NAE SharePoint](#):

- Anti-corruption & bribery policy
- Financial sanctions compliance, corporate policy statement, 2025
- Financial sanctions policy, 2025
- Guidance on sanctions monitoring (guidance to schools' Admissions and Finance Teams), 2025

*

Risk assessment checklist

The Bursary staff are to watch for the following warning signs. Should any of the following questions be answered 'yes', the Director of Finance & Operations must be informed:

	Potential red-flags	Ask ...	Yes/ No
1.	Transactions	Are payments unusual because of their size, frequency or the manner of their execution? For example: <ul style="list-style-type: none"> 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.	Bank account	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 illogical arrangements that make it unclear who is making the payment? For example: <ul style="list-style-type: none"> Is the payment coming from a variety of sources or payers? Is the payer seemingly unconnected to the student, parent or donor? 	
4.	Third party payments	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 student unclear? For example: <ul style="list-style-type: none"> Is the payment from someone who is not the parent's employer or a known relative of the student? 	
5.	Internet search	Are there any adverse media articles about the payer suggesting an involvement in criminal activities?	
6.	Erroneous payments	Has the school been asked to reverse a payment made because the payment was made in error? Has the school been asked to send a repayment to a person who is different from the original payer?	
7.	Country of residency	Is the parent resident in or have they recently relocated from, a high-risk country? You should ask the Director of Finance & Operations for the current list of high-risk countries.	

	Potential red-flags	Ask ...	Yes/ No
8.	PEP (Politically Exposed Person) ie, an individual performing a prominent public function	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.	Assets	Does it seem that a parent's assets are inconsistent with their known legitimate income?	
10.	Resources	Are a parent's funds made up of a disproportionate amount of private funding, bearer's cheques or cash, in relation to their socio-economic profile?	
11.	Identity	Is the payer difficult to identify?	
12.	Early or quick payments	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.	Donations	Is the payer offering a generous gift to the school as a donation or in response to an appeal?	
14.	False documents	Do any documents appear to be falsified, or withheld by the parent?	
15.	Representative	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?	

*

Flywire is a tuition fee payment processor and is used by more than 1,800 institutions worldwide and 60 independent schools 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 payments 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
www.flywire.com

*