All policies carrying the Bryanston logo apply equally to any other brands or operations of Bryanston including Bryanston Prep

ANTI-MONEY LAUNDERING POLICY

Bryanston could be used as a vehicle through which criminals seek to launder the proceeds of crime (Illicit Funds). Additionally, Bryanston, 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 Bryanston School and you personally, in respect of money laundering and associated activities. The purpose of this policy is to:

- provide a clear statement of Bryanston School's position regarding the prevention of financial crime;
- assist staff with identifying red flags that may be indicative of money laundering activities;
- reduce the risk of Bryanston 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 Bryanston 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 Bryanston School'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 Bryanston 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 Bryanston School

Bryanston starts with the premise that the people with whom it does business are not money launderers or terrorists. However, Bryanston School 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 Chief Operating Officer (COO).

Whilst Bryanston School is unlikely to have satisfied the threshold for committing a money laundering offence where the School 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 'red flags', that indicate a higher risk of potential money laundering activity, you must refer the concern to the COO who will consider what further steps or investigations are required before accepting the payment.

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

Identification and Verification
Before entering into any transaction with a person or organisation with whom the School has no previous transactions, the School needs to take reasonable steps to ascertain the identity of that person or organisation.

In the case of individuals, the key information is:

- Full name, including surname
- Residential address
- Date of birth
- Passport number including country of issue
- Nationality
- Citizenship
- Source of funds used to pay school fees e.g. parents' income/savings, family member, trust fund, bursary or scholarship etc.

Depending on whether particular risk factors are present, (see Annex 1) the School 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.

Copies of passports will be taken for all pupils joining the School and both parents are usually required to provide their name and residential address and to sign the School's Acceptance Form. As detailed above, copies of parents' passports should be taken to check their identity where any risk factors are present. Copies should not be retained but a note should be kept to evidence the checking process has taken place and the reason why (to include retaining a note of the fee payer's passport number and country of issue).

The School will consider the option of using commercial verification services This is particularly relevant to overseas jurisdictions where the school may have limited access to relevant databases and records.

In relation to organisations that are not already known to the School, staff will check 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.

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 School is increased where the School accepts payments in cash.

As part of a risk-based approach to the receipt of funds, all parents are encouraged to pay school fees through direct debit from a UK bank account.

Accordingly, it should be the exception that cash payments of more than £5,000 are accepted.

Staff should not accept payments in cash, in excess of, £5,000 in any circumstances. In exceptional cases the School may allow a larger payment to be made in cash. Before agreeing to accept a large cash payment, the COO or person nominated by the COO will consider the circumstances relating to the payment. The COO must obtain evidence to satisfy the School 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 COO must consider the explanation and information provided by the parent and decide whether the School is able to accept the cash payment. In each case, the COO 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 School must not accept the cash payment.

If the COO is not satisfied that the funds are clean, the COO must consider whether, in the circumstances the School should:

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

Refunds

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

Key areas of risk for Bryanston School

Money laundering can take many forms, but in relation to the School 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 non-exhaustive, and as a member of staff you should remain vigilant in relation to all payments the School receives.

Donations

Donations are a particular area of potential risk faced by the School. To mitigate the risk Bryanston School 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 School and its donors is essential for building trust and confidence.

Good due diligence will help to:

- assess any risks to Bryanston that may arise from accepting a donation or types of donations;
- ensure that it is appropriate for Bryanston to accept money from the particular donor;
- give Bryanston reasonable assurance that the donation is not from any illegal or inappropriate source,and;
- ensure that any conditions that may be attached to 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 1** to this policy.

The completed checklist must be provided to the COO 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 COO or their deputy immediately.

Requests for repayments

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, you must refer this to the COO promptly.

Charity Commission

When accepting payments or donations Bryanston School 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.

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

- **'identify'** who the School 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 School to be involved with;
- '**know what their specific business is with the School'** and have confidence that they will deliver what we want them to, and;
- '**watch out'** for unusual or suspicious activities, conducts or requests.

If Bryanston is not satisfied with the explanation or evidence provided to support these factors the School 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 School must carry out further investigations about the payer.

What warning signs should staff be alert to?

Annex 1 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 School's risk assessment when accepting payments. They are potentially relevant to all transactions and payments accepted by Bryanston School.

The School is not expected to consider every payment in detail against the red flag checklist and will consider payments on a risk basis. The COO has identified the payments listed below

as being payments that may expose Bryanston 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 Bryanston can accept the payment:

- For unsolicited or unexpected donations or cash payments of 5,000 or over
- payments from high-risk countries (See Annex 2)
- payments from PEPs (Politically exposed person – someone who has been entrusted with prominent public functions, or any immediate family member or close associate of such a person).

Countries that are considered to be high-risk countries are listed in **Annex 2.** These will be reviewed, and the list updated on a regular basis. If in doubt, you should ask the COO 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 School. You must promptly report any concerns to the COO or nominated person.

Reporting Suspicious Activity

This policy is separate from the School's procedures regarding grievances and whistleblowing. Rather, this procedure is to enable members of staff to express a legitimate concern regarding suspicions of money laundering or financial crime.

Bryanston School 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, the COO will act as the point of contact and, in their absence, the Compliance Officer is authorised to act as deputy. The function of the COO 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 Governors, annually or more frequently if requested, on the operation and effectiveness of the School's anti-money laundering procedures, and;
- keep this policy and related procedures under review.

What should staff do? - Disclosure Procedures

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 COO or their deputy.

Staff must make a report to the COO 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 e.g money or other property likely to be used for the purposes of terrorism.

If you have any concerns or suspicions relating to the COO, the same process should be followed but must be reported to the Head or Chair of the Finance and General Purposes Committee.

Your report should include as much detail as possible including:

- full available details of the people, 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 suspicious have been discussed with anyone and if so on what basi
- whether any aspect of the transaction(s) is outstanding and requires content to progressany other information that may help the COO judge the case for knowledge or suspicion of money laundering and to facilitate any external report

It is the School's policy, that following a disclosure to the COO you must follow any instructions provided. You must not make any further enquiries unless instructed to do so by the COO. 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 COO as they happen, unless and until the COO has confirmed that no report to the NCA and the local police is to be made.

If you identify a red flag in relation to any payment or proposed payment you must report your concerns to the COO or their deputy immediately.

Where you make a report to the COO or deputy you must not discuss your concerns with any other person, including other members of staff including senior leaders, pupils, parents or a donor as this could result in you, or the School, committing a secondary offence of prejudicing an investigation.

What must the COO do when a payment seems suspicious?

Where a member of staff identifies a red flag in relation to a payment the COO or nominated person must consider the relevant circumstances relating to the transaction that has raised the concern. The enquiries the COO or nominated person 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 COO will decide whether:

- the payment can be accepted
- further explanation or evidence as the legitimacy of the funds is required
- the School should submit a Suspicious Activity Report, and
- the School should make a report to the Charity Commission.

The COO will report any suspicions of money laundering activity, and how they have been managed, to the Finance & General Purposes Committee.

The COO 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 COO or deputy to have a reasonable suspicion or knowledge that the funds being used to make the payment may be Illicit Funds the COO must make a suspicious activity report (SAR) to the NCA and, where appropriate request consent to proceed with the transaction.

The COO will 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.

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 NCA to respond to the SAR has expired.

The COO will also consider whether the incident needs to be reported to the Charity Commission and, if so, will follow the procedures set out in the Schools Charity Commission Protocol.

Pupil Safety

The practice of pupils carrying large sums of money puts them at risk and should be actively discouraged. Any pupil travelling to the UK from outside the EU carrying in excess of 10,000 euros (or the equivalent or more in another currency), bankers drafts or cheques must complete a cash declaration form on arrival. If this is not completed or is completed incorrectly, the pupil may be subject to financial penalty. In addition, the HMRC has the

power to seize the money upon arrival if they have any suspicions about its source or purpose.

Training

Bryanston School will train relevant staff from time to time on how to limit the money laundering risks faced by the School, 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 COO or nominated person in the first instance.

Reviewed: February 2024
Reviewer: Finance Director
Next Review: September 2024
Author: COO

Annex 1

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 COO or deputy 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 COO or deputy.

	Potential red-flags	**Ask…**	**Yes/ No**
1.	**Transactions**	Are payments to the School 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? or making overpayments for no good reason? 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: Is the payment coming from a variety of sources or payers? Is the payer seemingly unconnected to the pupil, 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 pupil unclear?	

		For example, is the payment from someone who is not the parent's employer or a known relative of the pupil?	
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 that is different to the original payer?	
7.	**Country of residency**	Is the parent resident in or have they recently relocated from, a high-risk country? **See Annex 2** or ask the COO for the latest up to date list.	
8.	**PEP (Politically Exposed Person – broadly an individual who is 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 the funds being used bearer's cheques or cash?	
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.	**False documents**	Do any documents appear to be falsified?	
14.	**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?	

Annex 2

List of countries considered to have less rigorous processes in place to combat money laundering and terrorist financing.

This list was amended on 23rd February 2024 by the Money Laundering and Terrorist Financing (Amendment) (High-Risk Countries) Regulations 2022. The high-risk third countries are:

- Bulgaria
- Burkina Faso
- Cameroon
- Croatia
- Democratic People's Republic of Korea (DPRK)
- Democratic Republic of the Congo
- Haiti
- Iran
- Jamaica
- Kenya
- Mali
- Mozambique
- Myanmar
- Namibia
- Nigeria
- Philippines
- Senegal
- South Africa
- South Sudan
- Syria
- Tanzania
- Turkey
- Vietnam
- Yemen

Removed: Albania, Barbados, Cayman Islands, Gibraltar, Jordan, Panama, Uganda and United Arab Emirates.

Added: Bulgaria, Cameroon, Croatia, Kenya, Namibia, Nigeria, South Africa and Vietnam.

See also HM Treasury's advisory notice about risks posed by jurisdictions with unsatisfactory money laundering controls.

Staff must check with the Chief Operating Officer or deputy for the latest list.

Further, be aware that transactions with the following countries pose an increased risk:

- Syria
- South Sudan
- Yemen
- Myanmar
- Cuba
- Mali

- Iran
- DPRK
- Democratic Republic of Congo

With effect from 31 October 2023 HSBC will no longer process payments to or from Russia or Belarus.