ANTI-MONEY LAUNDERING POLICY

It ensures compliance with applicable laws and regulations, safeguarding the integrity and transparency of our institution

1ª Review: July 2025

Policy owner: Group Chief Financial Officer

Introduction and rationale

1.1 Changes to the legislation concerning money laundering around the world have broadened the definition of money laundering and increased the range of activities caught by the statutory framework. It is no longer merely an issue for banks and the financial sector but now applies to all companies including International Schools Partnership Limited, our subsidiaries and the schools operated by us. In order to combat the risk of money laundering and terrorist financing we need to implement anti-money laundering ("AML") and counter-terrorist financing ("CTF") policies and procedures.

If you have any knowledge or suspicions of money laundering or terrorist financing regarding any matter within our business please report this to your local Regional Finance Director ("RFD") in writin immediately. Please make the report confidentially and do not discuss this with anyone else (in particular any external party), as doing so could constitute a criminal offence. Further details on how to make a report can be found at section 6 below.

Your local RFD, in conjunction with the DCFOs as appropriate, will then consider whether to make an internal report to the global MLRO: Group Chief Finance Officer, Darren Mee (e-mail: dmee@ispschools.com).

MLRO means 'Money Laundering Reporting Officer' and is the ISP employee appointed to oversee ISP's compliance with its AML practices.

1. Scope of the Policy

1.1 This is a mandatory policy which applies to all ISP owned, controlled or managed entities and businesses (including the schools operated by us), as well as all ISP's directors, members, staff (including all employees, contractors, consultants, legal advisers, support staff, HR and operations staff), whether permanent or on fixed term or temporary arrangements and including those on work experience or other temporary placements ("ISP", "we" and "us").

1.2 This Policy is designed to reflect the AML and CTF legislation as well as best practice applicable to ISP globally. Where necessary, bespoke riders have been created for certain jurisdictions – these riders can be found at Annex A. This Policy is to be read in conjunction with those riders..

1.3 This Policy is designed to reflect the findings of ISP's latest AML and CTF risk assessment and forms a part of ISP's overall crime prevention model. This Policy will be reviewed regularly and may

be amended from time to time.

1.4 Any employee who breaches this Policy will face disciplinary action, in line with the local regional disciplinary procedure and local employment legislation and which could result in dismissal for gross misconduct depending on the gravity of the breach. Any non-employee or organisation which breaches this Policy may have their contract for services terminated with immediate effect.

2. Definition of money laundering

2.1 In short, money laundering is the process of making money generated by a criminal activity, such as drug trafficking or terrorist funding, appear to have come from a legitimate source. The money from the criminal activity is considered dirty, and the process "launders" it to make it look clean.

2.2 There are different pieces of legislation around the world that cover money laundering. Each of the money laundering offences revolve around the concept of "criminal property", which should be defined widely as any property; however, for the purposes of this Policy, offences relating to money laundering should be understood as follows:

• concealing, disguising, converting or removing criminal property from the country;
• entering into or becoming concerned in an arrangement which the person knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person;
• acquiring, using or having possession of criminal property;
• making a disclosure to a person which is likely to prejudice a money laundering investigation;
• failing to disclose knowledge or suspicion of money laundering (including making relevant internal and external reports).

2.3 Certain money laundering regulations apply to cash transactions in excess of specific amounts – please see our separate Cash Controls Policy for details on the specific cash limits in your jurisdiction.

3. Risks to which ISP may be exposed

3.1 As banks and financial services become more tightly regulated, criminals may look to what they see as softer targets in other sectors for opportunities to clean up money. To mitigate the risk of ISP becoming involved in money laundering, we have: (i) carried out a risk assessment that identifies and assesses the principal money laundering risks to which we are exposed; (ii) put in place this Policy to formally address those risks.

3.2 The following list sets out examples of 'red flag' activities that should arouse concern or suspicion

of money laundering or terrorist financing. In each of these instances ISP must apply "enhanced due diligence" ("EDD") procedures as set out in further detail below:

• any large cash payments (including a number of smaller cash payments that total a larger amount);
• cheques drawn from unusual sources;
• any secrecy, deceptiveness or conflicting information provided in respect of personal details such as name, identity, address and bank details;
• frequent or sizeable overpayments and requests for refunds (particularly to a different account or individual to the payer);
• payment of refundable tuition fees followed by a failure to take up a school place (particularly when accompanied by a request to send the refundable amount to a different bank account);
• use of agents who do notfitin with normal proceduresrelating to deposits and tuition fees;
• receipt of unexpected payments from third parties,the excess be transferred into a different account;
• the involvement of any politically exposed person ("PEP") and their associated persons in a business relationship - we need to be extra vigilant and careful when dealing with PEPs. A PEP is, broadly, any individual in a prominent public position whose position places them at greater risk of money laundering – examples of PEPs include:
• current and former senior official in the government or military (whether elected or not);
• senior member of a political party;
• senior executive of government owned commercial enterprise;
• family members of any of the above or someone who is known to be a close personal or professional associate of any of the above.

3.3 EDD may also be appropriate in respect of applicants from and transactions carried out in high risk countries (see the FATF high risk country registers and Annex B). Countries which are deemed to be high risk are subject to change. Any changes to the list of high risk countries maintained by FATF will be monitored by Group Legal and communicated to the relevant RFD, following which an approach to EDD will be agreed.

3.4 It should also be considered suspicious for a debt to be settled by a third party other than the person directly responsible for paying the student's fees. Whilst it is normal practice in some territories for tuition fees to be settled by a third party (e.g. grandparent, uncle, aunt), we need to understand the relationship between the student and the third party wishing to pay the student's fees (e.g. parent) and further information should be sought and due diligence carried out where necessary. ISP has prepared some further guidance on what activity may prompt further investigation in the 'Proceeds of Bribery and Corruption for Schools' briefing note.

4. Student and customer identification – "customer due diligence" ("CDD")

4.1 It is important that controls are in place to identify the student, tuition fee payer, customer or other third party dealing with the school. CDD must always be carried out on the basis of reliable documents and information. Examples of supporting documentation include (but are not limited to)

the following. Students:

• Passport or other government-issued ID;
• Visa/proof of residency;
• Birth certificate.

Parents and other person(s) paying tuition fees (obtain passport or other government- issued ID plus one or more others from the list below):

• Passport or other government-issued ID;
• Visa/proof of residence;
• Tax identification;
• Bills/invoices to support proof of name and address;
• Letter(s) explaining the relationship with the student.
Payments received by companies :
• To be determined on a case-by-case basis, Group Legal to be consulted on what CDD documents should be obtained. You can use the following email address for this purpose: ISPCompliance@ispschools.com

4.2 CDD checks should be carried out before establishing a new business relationship. No monies may be accepted from any person until all CDD (and, where necessary, EDD) checks have been completed. ISP must take a risk-based approach to any particular fact patterns and apply CDD and EDD checks accordingly.

4.3 In addition to the measures set out above, the RFD and MLRO (this is ISP's Group CFO – see details below) should both be notified of any transactions or relationships involving PEPs.

5. Enhanced Due Diligence

5.1 Where one or more red flag fact patterns (including those at section 3.2 above) have been identified, your local RFD will need to apply EDD measures to be determined in conjunction with Group Legal. This may include the following:

• obtaining additional information about the customer (including, where the customer is a company, its corporate structure and any beneficial owners) from independent sources;
• obtaining information relating to the source of wealth of the customer and beneficial owner;
• obtaining additional information and supporting documents in respect of the source of funds to be used in a transaction;
• conducting further research and adverse media screening in relation to the customer or beneficial owner;
• conducting additional screening of persons associated with the customer (such as directors and

instructing persons) and known associates of the beneficial owner; and
• conducting enhanced ongoing monitoring of the business relationship.

5.2 Note that, unless specified otherwise, the additional information requirements set out in section 5.1 can be obtained either from the customer or independent sources, or a combination of both.

6. Making internal AML/CTF reports

6.1 When you know or suspect that a money laundering or terrorist financing activity is taking or has taken place, you must disclose this immediately in writing to your local RFD ("Internal Disclosure Report") (see section 6.2 below for the information to include). The RFD may then recommend and oversee the carrying out of further EDD measures (see section 5 above) and/or recommend that you make a written internal disclosure report to ISP's MLRO (an "MLRO Report"). The MLRO nominated at ISP is the Group CFO, Darren Mee (e-mail: dmee@ispschools.com).

6.2 An Internal Disclosure Report to the RFD should contain as much detail as possible including:

• full available details of the people and companies involved and all staff members who have dealt with the suspected transaction;
• reasons as to why you have knowledge or suspicion that money laundering or terrorist financing may take or have taken place;
• dates of the transactions, amounts involved and method of transfer of money or assets; and any other information that may help the MLRO judge the case for knowledge or suspicion of money laundering.

6.3 If and when any person makes an MLRO Report, that person should not make any further enquiries unless requested by the RFD or MLRO. Following a report to the MLRO, any inbound enquiries from a person suspected of money laundering (for example, asking for confirmation that the fees have been settled) should be reported to the MLRO prior to any response being given.

6.4 No person should discuss their knowledge or suspicion (including the fact that an Internal Disclosure Report or an MLRO Report has been made) with the person whom they know or suspect is involved in money laundering and/or terrorist financing. This will help to avoid making a disclosure which may prejudice a money laundering investigation, which is a criminal offence in most jurisdictions.

7. Controls to mitigate risk

7.1 Refunds of payments must only be made by the same method and to the same account as the original payment was made, provided prior approval from the RFD has been obtained. For the

avoidance of doubt, no refunds should be made in cash.

7.2 Any individual who overpays and requests a refund more than once must be promptly flagged to the RFD and subject to EDD.

7.3 In the event of payment by credit or debit card being rejected,the reason should be checked with the card provider prior to accepting an alternative card with different details.

7.4 Where fees paid in advance for foreign students who have subsequently been refused a visa are refundable in accordance with the application and/or enrolment documents, such refunds may only be provided where appropriate documentary evidence is available to demonstrate the circumstances for such visa refusal. Refunds must only be made to the person making the original payment or, where required, by way of transfer to a new school.

8. Duties of the Money Lending Reporting Officer (MLRO)

8.1 The MLRO will consider the MLRO Report and any other available internal information considered relevant, such as:
• reviewing other transaction patterns and volumes;
• the length of any business relationship involved;
• the number of any one-off transactions and linked one-off transactions; and
• any identification evidence held,

and undertake such other reasonable enquiries he/she thinks appropriate in order to ensure that all available information is taken into account in deciding whether a report to the relevant authorities are required. The MLRO may also need to discuss the report with the employee.

8.2 The MLRO will consider whether to make an external report to the relevant authority or authorities.

9. Records and training

9.1 All CDD and EDD documentation, including all Internal Disclosure Reports and MLRO Reports and associated documentation (e.g. the MLRO's internal correspondence regarding MLRO Reports), must be retained securely for five years from the date it was obtained.

9.2 As part of their formal onboarding, all new hires may be directed to complete an AML and CTF training module and to attest to having read the firm's financial crime policies and procedures. Such new hires will not pass probation without successfully completing the course.

9.3 Staff at ISP will be required to complete ISP's AML training module at least every two years.

Certain individuals in key functions (such as finance, procurement, HR, management) or who have otherwise been allocated responsibility to carry out CDD and EDD checks, as well as RFDs and the MLRO, are required to complete ISP's AML and CTF training module annually.

Annex A – Jurisdiction-specific riders

Brazil

• It is particularly important to carry out due diligence on suppliers and government contracts in Brazil.

Canada

• Certain provinces also administer laws and regulations in relation to AML activity in the jurisdiction. By way of example, the British Columbia government has published a policy requiring independent schools located in British Columbia to establish an AML and cash payment policy addressing certain enumerated items. However, we are not aware of any similar policies or requirements in the province of Ontario (where both ISP schools are located).

Malaysia

• It is a requirement under section 66B(3)(d) of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 to disclose immediately to the Inspector General of Police the existence of property in one's possession or control that they have reason to believe is owned or controlled by or on behalf of a specified entity, and information about a transaction or proposed transaction in respect of such property.

Panama

• All accounting records for ISP entities operating in Panama must be retained, including for seven years following closure of any relevant business in Panama. USA

• FinCEN has recently implemented a Beneficial Ownership Information reporting requirement that may be applicable to ISP. As of 1 January 2024, the rule requires "domestic reporting companies" and "foreign reporting companies" to report their beneficial owners to FinCEN unless an exemption applies. A "domestic reporting company" is generally a legal entity created under the law of any US state. A "foreign reporting company" is a legal entity created under the laws of any non-US country and registered to do business with a state in the US.

• As a result, if ISP intends to incorporate an entity in the US for the purposes of operating a school in the US or intends to register to do business in a US state, it will need to report its beneficial owners to FinCEN unless an exemption applies. The only exemption that might apply to ISP is the "large operating company" exemption, which applies to companies that: (i) employ 20 or more full-time employees in the US; (ii) have an operating presence at a physical location in the US; and (iii) report more than USD 5,000,000 in gross receipts or sales on its US tax return. Under the FinCEN reporting requirements, a beneficial owner is any individual who, directly or indirectly, either exercises substantial control over the reporting company, or owns or controls at least 25% of the ownership

interests of the company.

Vietnam

• ISP should ideally only receive bank transfers (i.e., no cash payments).

Annex B – High-risk jurisdictions in which ISP operates (as of 30/05/2024)

Vietnam