EL ALTILLO INTERNATIONAL SCHOOL

PART OF ISP SCHOOLS

ANTI MONEY LAUNDERING POLICY

Publication date:

Review date: November 2026

Policy owner: Group Finance Director

Introduction and rationale

Changes in legislation relating to money laundering around the world have broadened the definition of money laundering and increased the range of activities covered by the legal framework. It is no longer an issue affecting only banks and the financial sector; it now applies to all businesses, including International Schools Partnership Limited, our subsidiaries and the schools we operate. To combat the risk of money laundering and terrorist financing, we must implement anti-money laundering (AML) and counter-terrorist financing (CTF) policies and procedures.

If you become aware of or suspect money laundering or terrorist financing in connection with any matter within our business, report it immediately in writing to your local Regional Finance Director (RFD). Make the report confidentially and do not discuss the matter with anyone else (particularly external third parties), as doing so could constitute a criminal offence. Further details on how to make a report are set out in section 6 below.

Your local RFD, together with the DCFOs where appropriate, will then consider whether to submit an internal report to the Global Money Laundering Reporting Officer (MLRO): the Group Finance Director, Darren Mee (email: dmee@ispschools.com).

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

1. Scope of the policy

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

1.2 This policy is designed to reflect AML and CTF legislation and best practice applicable to ISP globally. Where necessary, additional clauses have been created for specific jurisdictions; these can be found in Appendix A. This policy should be read together with those additional clauses.

1.3 This policy is designed to reflect the findings of ISP's latest AML and CTF risk assessment and forms part of ISP's overall crime prevention framework. It will be reviewed periodically and may be amended from time to time.

1.4 Any employee who breaches this policy will face disciplinary action in accordance with the relevant local regional disciplinary procedure and local employment law, which could result in dismissal for gross misconduct, depending on the seriousness of the breach. Any person or organisation not employed by the business that breaches this policy may have their service contract terminated with immediate effect.

2. Definition of money laundering

2.1 In summary, money laundering is the process of making money generated by criminal activity, such as drug trafficking or terrorist financing, appear to come from a legitimate source. Money generated by criminal activity is considered dirty, and the process 'launders' it so that it appears clean.

2.2 Different laws around the world regulate money laundering. Each money laundering offence revolves around the concept of 'criminal property', which should be defined broadly as any property. However, for the purposes of this policy, money laundering offences should be understood as follows:

- concealing, disguising, converting or removing criminal property from the country;
- becoming involved in or participating in an arrangement which a person knows or suspects facilitates (by any means) the acquisition, retention, use or control of criminal property by or on behalf of another person;
- acquiring, using or possessing criminal property;
- disclosing information to a person which may 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 above specified amounts. Please refer to our Cash Handling Policy for further information 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 heavily regulated, criminals may look for what they consider to be easier targets in other sectors in order to launder money. To mitigate the risk of ISP becoming involved in money laundering, we have: (i) carried out a risk assessment identifying and evaluating the main money laundering risks to which we are exposed; and (ii) implemented this policy to formally address those risks.

3.2 The following list gives examples of 'suspicious' activities which should raise concerns or suspicion of money laundering or terrorist financing. In each of these cases, ISP must apply the Enhanced Due Diligence ('EDD') procedures described in more detail below:

- any large cash payment (including several smaller cash payments which add up to a larger amount);
- cheques issued from unusual sources;
- any secretive, misleading or contradictory information provided in relation to personal details such as name, identity, address and bank details;
- frequent or substantial overpayments and requests for refunds (particularly to an account or person different from the payer);
- payment of refundable school fees followed by a failure to take up a school place (particularly where accompanied by a request for the refundable amount to be sent to a different bank account);
- use of agents which does not comply with normal procedures relating to deposits and school fees;
- receipt of unexpected payments from third parties, with the excess transferred to a different account;
- the involvement of any politically exposed person ('PEP') and their associates in a business relationship. We must be very alert and cautious when dealing with PEPs. A PEP is generally any person who holds a prominent public position and whose role exposes them to a higher risk of money laundering. Examples of PEPs include:
- current and former senior government or military officials (elected or otherwise);
- senior members of a political party;
- senior executives of state-owned commercial enterprises;
- family members of any of the above, or persons known to be close associates of any of them, whether personally or professionally.

3.3 EDD may also be appropriate for applicants from high-risk countries and transactions carried out in such countries (see the FATF high-risk country lists and Appendix B). Countries considered high risk are subject to change. Any changes to the list of high-risk countries maintained by the FATF will be monitored by the Group Legal Department and communicated to the relevant RFD, after which an EDD approach will be agreed.

3.4 It will also be considered suspicious if a debt is settled by a third party other than the person directly responsible for paying the student's fees. Although in some territories it is common for tuition fees to be paid by a third party (for example, grandparents, uncles or aunts), we must understand the relationship between the student and the third party wishing to pay the fees (for example, the parents) and, where necessary, obtain further information and carry out due diligence. ISP has produced additional guidance on activities which may lead to further investigation in the briefing note 'Proceeds of Bribery and Corruption for Educational Institutions'.

4. Identification of students and customers: 'Customer Due Diligence' (CDD)

4.1 It is important to have controls in place to identify the student, the fee payer, the customer or other third parties 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 identity document;
- Visa/proof of residence;
- Birth certificate.

Parents and other fee payers (obtain a passport or other government-issued identity document, in addition to one or more of the following):

- Passport or other government-issued identity document;
- Visa/proof of residence;
- Tax identification;
- Bills/receipts showing name and address;
- Letter(s) explaining the relationship with the student.

Payments received from companies:

- This will be determined on a case-by-case basis, consulting the Group Legal Department on the CDD documents to be obtained. The following email address may be used: ISPCompliance@ispschools.com.

4.2 CDD checks must be carried out before establishing a new business relationship. No money must be accepted from anyone until all CDD checks (and, where necessary, EDD checks) have been completed. ISP must adopt a risk-based approach to any particular pattern and apply CDD and EDD checks accordingly.

4.3 In addition to the measures set out above, the RFD and the MLRO (who is the ISP Group Finance Director; see further details below) must be notified of any transaction or relationship involving a PEP.

5. Enhanced Due Diligence

5.1 Where one or more patterns of facts constituting red flags have been identified (including those in section 3.2 above), your local RFD must apply EDD measures to be determined jointly with the Group Legal Department.

This may include:

- obtaining additional information about the customer (including, where the customer is a company, its corporate structure and any beneficial owner) from independent sources;
- obtaining information about the source of the customer's and beneficial owner's wealth;
- obtaining further information and supporting documents about the source of funds to be used in a transaction;
- carrying out further investigations and an adverse media review in relation to the customer or beneficial owner;
- carrying out further analysis of persons associated with the customer (such as directors and persons giving instructions) and the beneficial owner's known partners; and
- carrying out ongoing enhanced monitoring of the business relationship.

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

6. Internal AML/CTF reporting

6.1 Where you know or suspect that money laundering or terrorist financing is taking place or has taken place, you must immediately report it in writing to your local RFD ('Internal Disclosure Report') (see section 6.2 below for the information to be included). The RFD may then recommend and oversee the implementation of further EDD measures (see section 5 above) and/or recommend that a written internal disclosure report be submitted to ISP's MLRO (an 'MLRO Report'). ISP's appointed MLRO is the Group Finance Director, Darren Mee (email: dmee@ispschools.com).

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

- all available details of the individuals and companies involved and all staff members who have dealt with the suspicious transaction;
- the reasons why you know or suspect that money laundering or terrorist financing may be taking place or may have taken place;
- the dates of the transactions, the amounts involved and the method of transferring money or assets; and any other information which may help the MLRO assess the case on the basis of knowledge or suspicion of money laundering.

6.3 If anyone submits a report to the MLRO, they must not make any further enquiries unless requested to do so by the RFD or MLRO. After submitting a report to the MLRO, any enquiry received from a person suspected of money laundering (for example, asking for confirmation that fees have been paid) must be referred to the MLRO before any response is given.

6.4 No one must discuss their knowledge or suspicion (including the fact that an Internal Disclosure Report or MLRO Report has been submitted) with the person they know or suspect to be involved in money laundering and/or terrorist financing. This will help avoid making a disclosure which could 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 using the same method and to the same account from which the original payment was made, provided prior approval has been obtained from the RFD. For the avoidance of doubt, refunds must not be made in cash.

7.2 Anyone who overpays and requests a refund more than once must be flagged to the RFD immediately and subject to EDD.

7.3 If a credit or debit card payment is declined, the reason must be checked with the card provider before accepting an alternative card with different details.

7.4 Where fees paid in advance by foreign students who are subsequently refused a visa are refundable under the application and/or enrolment documents, refunds may only be made where appropriate documentary evidence of the circumstances of the visa refusal is available. Refunds will only be made to the person who made the original payment or, where necessary, by transfer to a new school.

8. Responsibilities of the Money Laundering Reporting Officer (MLRO)

8.1 The MLRO will consider the MLRO Report and any other relevant internal information available, such as:

- a review of other transaction patterns and volumes;
- the duration of any business relationship involved;
- the number of one-off transactions and linked one-off transactions; and
- any identification evidence held,

and will carry out any further reasonable investigations considered appropriate to ensure that all available information is taken into account when deciding whether a report to the relevant authorities is necessary. The MLRO may also need to discuss the report with the employee.

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

9. Records and training

9.1 All documentation relating to CDD and EDD, including all Internal Disclosure Reports and MLRO Reports, together with associated documentation (for example, the MLRO's internal correspondence relating to MLRO Reports), must be kept securely for five years from the date it was obtained.

9.2 As part of their formal onboarding, all new employees may be required to complete an AML and CTF training module and certify that they have read the company's financial crime policies and procedures. Such new employees will not pass their probationary period unless they successfully complete the course.

9.3 ISP staff must complete ISP's AML training module at least every two years. Certain individuals in key roles (such as finance, procurement, HR and management), or those assigned responsibility for carrying out CDD and EDD checks, as well as RFDs and the MLRO, must complete ISP's AML and CTF training module annually.

Appendix: Jurisdiction-specific additional clauses

Brazil

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

Canada

- Some provinces also administer laws and regulations relating to AML activity in the jurisdiction. For example, the Government of British Columbia has published a policy requiring independent schools located in British Columbia to establish an AML and cash payment policy addressing certain specified matters. However, we are not aware of any similar policy or requirement in the province of Ontario (where ISP's two schools are located).

Malaysia

- Section 66B(3)(d) of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 requires the immediate reporting to the Inspector General of Police of the existence of property in the possession or under the control of a person who has reason to believe that it is owned or controlled by, or on behalf of, a specified entity, as well as information about a transaction or proposed transaction relating to such property.

Panama

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

United States

- FinCEN has recently implemented a beneficial ownership reporting requirement which may apply to ISP. From 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 laws 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 in a US state.
- Accordingly, if ISP intends to incorporate an entity in the United States to operate a school there, or to register to do business in a US state, it must report its beneficial owners to FinCEN unless an exemption applies. The only exemption which may apply to ISP is the 'large operating company' exemption, which applies to companies that: (i) employ 20 or more full-time employees in the United States; (ii) have an operating presence at a physical location in the United States; and (iii) report more than USD 5,000,000 in gross receipts or sales in their US tax return. Under FinCEN's reporting requirements, a beneficial owner is any individual who, directly or indirectly, exercises substantial control over the reporting company or owns or controls at least 25% of the company's ownership interests.

Vietnam

- Ideally, ISP should only receive bank transfers (i.e. no cash payments).