

ANTI-BRIBERY AND CORRUPTION POLICY

Policy owners: Group Head of Legal and Group Head of People Operations

1. Introduction and rationale

1.1 It is our policy to conduct all of our business in an honest and ethical manner. We take a zero tolerance approach to bribery and corruption and are committed to acting professionally, fairly and with integrity in all of our business dealings and relationships, in addition to implementing effective anti-bribery and corruption ("ABC") systems, as set out in this global policy (the "**Policy**"). We take our legal responsibilities seriously and will uphold all applicable ABC laws in the countries in which we operate.

1.2 The purpose of this Policy is to:

- (i) set out the ABC responsibilities of ISP and those working for us and on our behalf; and
- (ii) provide guidance to those subject to this Policy on how to recognise and address ABC issues.

All forms of bribery and corruption are strictly prohibited, and you should have particular regard to the local ABC laws of the country or countries in which you work. In ISP's countries of operation, individuals found guilty of bribery or corruption can be subject to imprisonment and/or a fine.

If you are offered a bribe, or are asked to make one, or if you believe or suspect that any bribery, corruption or other breach of this Policy has occurred or may occur, you must notify your line manager and report it in accordance with the Whistleblowing Policy as soon as possible. If you are unsure about whether a particular act constitutes bribery or corruption, please consult with the Group Head of People Operations or the Group Head of Legal.

2. Scope of the Policy

2.1 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**").

2.2 This Policy is designed to reflect the ABC 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.

2.3 This Policy is designed to reflect the findings of ISP's latest ABC 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.

2.4 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.

3. Definition of bribery

3.1 Bribe means a financial or other inducement or reward for action which is illegal, unethical, a breach of trust or improper in any way. Bribes can take the form of money, gifts, loans, fees, hospitality, services, discounts, the award of a contract or any other advantage or benefit.

3.2 Bribery includes offering, promising, giving, accepting or seeking a bribe.

3.3 Corruption means the abuse of power or position for private gain.

4. Bribery offences

4.1 To prevent the commission of bribery and corruption offences, you (or someone acting on your behalf) must not engage in bribery or corruption – this includes the behaviours listed below. For the purposes of these offences the terms "give" and "receive" should be read widely to include soliciting, requesting, offering, accepting, promising and any other similar terms:

- give or receive any payment, gift, hospitality, undue advantage or other benefit in the expectation or hope that: (i) a business advantage will be received in return; or (ii) this shall reward any business advantage already received;
- give or receive any payment, gift, hospitality, undue advantage or other benefit from a third party that you know or suspect is offered with the expectation that we will provide a business advantage to them or anyone else in return, or where any business advantage has already been provided;
- give or receive any payment, gift, hospitality, undue advantage or other benefit to or from a government official or representative in any country (domestic or foreign) to facilitate or expedite a routine or necessary procedure (sometimes called a facilitation payment) or to cause the government official or representative to carry out, omit, delay or improperly perform any actions relating to their official functions;
- on the basis of your influence or position, or pretending to have an influence or position: give or receive any promise, payment, gift, hospitality, undue advantage or other benefit from a third party that you know or suspect is offered with the expectation that you will use your influence or position to provide a business advantage to them or anyone else in return;
- on the basis of violence or threats, give or receive any payment, gift, hospitality, undue advantage or other benefit from a third party;
- dispose of any of ISP's assets or assume obligations which could cause a detriment to ISP;
- conceal (for example by falsifying accounts) or fail to report any instances of bribery or corruption;
- threaten or retaliate against another person who has refused to offer or accept a bribe or who has raised concerns about possible bribery or corruption;
- engage in any other activity that may cause a breach of this Policy; or
- fail to prevent bribery or corruption by failing to have in place adequate policies or procedures designed to prevent relevant persons committing bribery or corruption.

5. Gifts and hospitality

5.1 Many organisations may give gifts (which includes the payment of expenses) and provide hospitality to build relationships and to market their business. Hospitality would normally include entertaining, meals and tickets to events. If the host does not attend the hospitality then it should be considered a gift rather than hospitality. Organisations may also pay expenses for a prospective client to visit part of the company or to attend a conference or event.

5.2 There can be significant risks around receiving or giving gifts and hospitality. Gifts and hospitality are often part of business culture and it can be difficult for personnel (i.e., employees and non-employees) to know what is appropriate in terms of giving and receiving gifts and hospitality. Gifts and hospitality can be used to influence and corrupt third parties and, on occasion, to manoeuvre personnel into a position of obligation.

5.3 This Policy does not prohibit the giving or accepting of reasonable and appropriate hospitality for legitimate purposes such as building relationships, maintaining our image or reputation, or marketing our products and services. As a group, however, we seek to prevent the giving and receiving of gifts and hospitality if it might influence or be perceived to influence a business advantage.

5.4 We recognise that practice may vary between the regions in which we operate and, as a general rule, you should determine whether the gift or hospitality is reasonable and justifiable in the circumstances. When giving or receiving gifts, hospitality or payments you therefore should consider:

- The purpose of the gift or hospitality – is it intended to cement good relations or is it intended as some form of inducement or reward for any preferential treatment (for example, during contractual negotiations or a tender process)? In the latter case, the gift or hospitality will not be appropriate.
- Is the recipient given the impression that they are under some obligation to confer business as a result of accepting the gift or hospitality?
- Is the gift or hospitality reasonable or is it lavish / extravagant? A gift or hospitality will not be appropriate if it is unduly lavish or extravagant.
- Is a record made of the gift and the cost entered into the accounts?

5.5 Gifts must be of an appropriate type and value depending on the circumstances and taking account of the reason for the gift. Gifts must not include cash or cash equivalent (such as vouchers) or be given in secret. Gifts should be given in the name of ISP or the relevant school, not in the name of any particular individual.

5.6 This Policy does not prevent the giving or receipt of promotional items such as branded pens, calendars or stationery that bear the company name or logo of another organisation, provided that these have no significant financial value and are given to or accepted from existing clients, suppliers or business partners.

6. Other forms of payment

6.1 Reimbursing a third party's expenses or accepting an offer for our expenses to be reimbursed (such as travel costs to attend a business meeting) would not usually constitute bribery, provided the payment is for genuine and reasonable business expenses. Payments in excess of this are not acceptable.

6.2 We do not make contributions to political parties or candidates.

7. Global operational requirements

7.1 Senior management in each country should ensure it implements this Policy without modification and stays up-to-date with regulatory developments in the relevant jurisdiction in order to mitigate ABC risks. We recognise that certain countries of operation may have additional ABC requirements and/or recommendations for best practice and these are reflected in the bespoke riders at Annex A. This Policy is to be read in conjunction with those riders.

7.2 ISP has implemented further steps that it deems necessary in order to prevent the commission of bribery and corruption related offences, including:

- regular staff training on compliance matters;
- a code of ethics and code of conduct;
- due diligence exercises to the extent appropriate in respect to third parties (i.e., customers, suppliers, service providers and government contracts);
- additional internal controls designed to identify and prevent financial crime (including ABC) risks, monitor compliance with this Policy and enforce sanctions for any breaches;
- internal procedures for whistleblowing (in line with the Whistleblowing Policy);
- procedures to enable the detection and correction of any failures and updating the controls based on the same or ISP's change of circumstances; and
- relevant reporting requirements to local authorities.

8. Your responsibilities and how to report and raise concerns

8.1 ISP promotes a culture of honesty and transparency in all of its practices. The prevention, detection and reporting of bribery and other forms of corruption are the responsibility of all those working for us or under our control. You are required to avoid any activity that might lead to, or suggest, a breach of this policy. If you fail to comply with this Policy, this constitutes a disciplinary offence and will be dealt with in accordance with ISP's disciplinary procedure. Depending on the gravity of the offence, this may be treated as gross misconduct in accordance with ISP's disciplinary procedure and could render you liable to immediate dismissal in line with your local disciplinary procedure and criminal sanctions.

8.2 If you give or receive any gift or hospitality you must report this to your line manager and RFD either before you give or upon receipt of the gift or hospitality (as the case may be). You must also provide details of the nature of the gift, its estimated value and the identity of the sender. Any line manager in receipt of any such report shall enter the relevant details on the register of gifts and hospitality referenced in section 8.5 below.

8.3 If you are offered a bribe, or are asked to make one, or if you believe or suspect that any bribery, corruption or other breach of this Policy has occurred or may occur, you must notify your line manager and RFD or report it in accordance with the local Whistleblowing Policy as soon as possible. If you are unsure about whether a particular act constitutes bribery or corruption, please consult with the Group Head of People Operations or the Group Head of Legal. You can use the following email address for this purpose: ISPCompliance@ispschools.com

8.4 Once details have been lodged with the RFD it then becomes the RFD's responsibility to document the meeting with the employee, have the contents verified by all in the meeting and bring it to the attention of the Divisional CFO and Group Legal with immediate effect so as to decide the necessary actions and next steps.

8.5 ISP expects each RFD to be responsible for the maintenance of a register of gifts and hospitality for his or her region (including for each school). The RFD may delegate the task of completing such registers to members of the regional team or the principal in respect of each School, but the RFD will have ultimate responsibility for their upkeep and maintenance. The Head of Group Legal will be responsible for the maintenance of a register of gifts and hospitality in respect of group activities. The Head of People Operations may conduct a 'spot check' review of the gift and hospitality registers to ensure compliance.

8.6 Any corporate hospitality should be approved by an employee's line manager in advance.

9. Records and training

- 9.1 You must declare and keep a written record of all gifts and hospitality given or received. All records (including accounts and invoices) relating to dealings with third parties (such as suppliers and clients) should be prepared with accuracy and completeness. Accounts must not be kept "off-book" to facilitate or conceal improper payments. ISP shall retain all such documentation securely for five years from the date it was obtained.
- 9.2 As part of their formal onboarding, new hires may be directed to complete an ABC 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 ISP staff will be required to complete ISP's ABC training module at least every two years. Certain individuals in key functions (such as finance, procurement, HR, management) are required to complete ISP's ABC training module annually.

Annex A – Jurisdiction-specific riders

Canada

- In addition to the elements specified at section 7.3 above, the compliance programme should include specific procedures for hiring foreign agents or establishing partnerships abroad. Namely, this should include carrying out and documenting due diligence, which considers whether the foreign party:
 - is reputable and qualified; and
 - does not employ foreign officials or have any links to government.Foreign parties should also be required to sign agreements that they will comply with all relevant ABC laws. Oversight should be maintained over the foreign entity.
- Federal, provincial and local Canadian lobbying laws require certain types of communication (for example communications related to the development of public policy and the awarding of public contracts or grants) with public office holders to be reported. Senior Management should remain aware of and comply with any such requirements.

Chile

- The internal compliance programme is known as a crime prevention model in Chile. In addition to the elements specified at section 7.3 above, effective crime prevention models should include:
 - appointing a prevention supervisor with sufficient means, powers, and independence to perform their duties; and
 - procedures for the administration and auditing of financial resources in ISP, including internal administrative sanctions.The model must also be tailored to ISP and its activities, and must be an integral part of ISP's business structure and operations in Chile.

Colombia

- In addition to the elements specified at section 7.3 above, the internal compliance programme should include:
 - the appointment of compliance officers (in order to prevent ABC risks); and
 - requirements around business transparency and ethics (in order to prevent ABC risks).
- Assess and (where relevant) comply with the obligations imposed by the Colombian province(s) in which ISP operates.

India

- In addition to the elements specified at section 7.3 above, the internal compliance programme should include systems to conduct due diligence through monitoring financial records.

Italy

- The internal compliance programme should include the implementation of a "231 Model" (being an anti-corruption compliance model). The model must be appropriate for preventing the commission of ABC offences, and the following measures (in addition to those specified in section 7.3 above) should be put in place:
 - appointing an independent and autonomous supervisory body to have oversight of the model;
 - identifying methods to manage financial resources to prevent ABC offences from being committed;
 - ensuring there is adequate internal communication in respect to ABC; and
 - implementing adequate sanctions for failure to comply with the model.

Malaysia

- In addition to the elements specified at section 7.3 above, the internal compliance programme should include procedures which implement the "TRUST Principles":
 - top level commitment;

- risk assessment;
- undertake control measures;
- systematic review, monitoring and enforcement; and
- training and communication.

Mexico

- In addition to the elements specified at section 7.3 above, the internal compliance programme should be accompanied by an integrity policy, to manage exposure to corruption and finance-related crimes. The programme should include:
 - a manual of organisation and proceedings, outlining all functions/responsibilities and setting out the chain of command and leadership structure;
 - control, monitoring and audit systems, which must be adequate and effective for periodically reviewing compliance within the organisation, in addition to exercising proper organisational control to prevent ABC offences;
 - "denouncing systems", which must be adequate and provide clear disciplinary procedures, including consequences;
 - HR policies, which should be effective in avoiding the hiring of individuals who may impact ISP's integrity. Such policies must not enable discrimination on the basis of ethnicity, nationality, gender, age, disabilities, social status, health status, religion, political opinion, sexual orientation, marital status, or any other basis that compromises human dignity or curtails human rights and liberties; and
 - transparency and publicity measures, which must ensure the transparency and publicity of ISP's interests at all times.

Morocco

- In addition to the elements specified at section 7.3 above, the internal compliance programme should include implementing decisions on the freezing of assets and transactions.

Panama

- Ensure all know your client forms requested by service providers of ISP (such as local banks or resident agents) are kept up to date.

Peru

- In addition to the elements specified at section 7.3 above, the internal compliance programme should include:
 - appointing a compliance officer who is responsible for ISP's prevention functions, and acts with autonomy and independence; and
 - disseminating and providing periodic training on the prevention model.

Poland

- "Persons holding public functions" (including employees of an organisational unit with access to public funds, such as a school director) are subject to the following requirements and restrictions:
 - they may not be a member of the governing body in commercial companies, or work/act on behalf of business entities, if the objectivity of their role is called into question;
 - they cannot hold more than 10% of the shares in commercial companies or conduct their own business activities; and
 - they must submit asset declarations, including assets under marital joint ownership.

Spain

- In addition to the elements specified at section 7.3 above, the internal compliance programme should require the appointment of an independent compliance officer or committee with the power to supervise the risk-prevention model.
- As a matter of good practice, due diligence should focus on identifying clients, assessing the

reasons behind transferring money, and maintaining knowledge of the business and market. By way of example, actions taken when carrying out due diligence should include asking questions about management, obtaining reports on internal investigations and reviewing internal policies/procedures relating to corruption, fraud or money laundering.

Switzerland

- In addition to the elements specified at section 7.3 above, the internal compliance programme should include the following:
 - appointing a compliance officer; and
 - applying the International Standardisation Organisation standard 37001 on anti-bribery management systems.

United Kingdom

- In addition to the elements specified at section 7.3 above, the internal compliance programme should implement the following:
 - senior management should be committed to preventing bribery by associated persons and should foster a culture in which bribery is never acceptable; and
 - ensure that the bribery prevention policies are embedded and understood throughout the organisation through internal and external communication (including training) which is proportionate to the bribery risks they face.

United States of America

- Comply with the beneficial ownership information reporting requirement. This entails reporting ISP's beneficial owners to FinCEN unless an exemption applies. The applicability of this requirement and exemptions to ISP should be periodically assessed.

Vietnam

- As a matter of best practice, any money or fees should be received by ISP via bank transfer, to ensure transparency in relation to the identity of the transferor and the amount of money received.