Whistleblowing procedure

25 March 2024

TABLE OF CONTENTS

1. DECLARATION 1
2. ABOUT THIS PROCEDURE 1
3. SCOPE OF APPLICATION 2
4. DEFFINITION OF WHISTLEBLOWING 3
5. RESPONSIBILITY 3
6. PROCEDURE FOR REPORTING INTERNALLY 4
7. OTHER REPORTING CHANNELS 9
8. DOCUMENTATION AND DATA PROTECTION 9
9. CONFIDENTIALITY 10
10. TRAINING 11
11. PROTECTION OF WHISTLEBLOWERS AND MEASURES AGAINST RETALIATION 11
12. DISCIPLINARY MEASURES AND SANCTIONS 12
13. LEGAL ACTIONS 13
14. PROCESS REVIEW 13
15. ANY QUESTIONS? 13

1. DECLARATION

The International School of Luxembourg, A.s.b.l., having its registered office at L-1430 Luxembourg, 36, Boulevard Pierre Dupong, registered with the Trade and Companies Register under number F398 (the **"School**"), **intends to conduct its business with honesty, integrity and in accordance with its values and expected standards of behaviour.** No breach of Luxembourg or European law will be tolerated, at any level. The School will also not tolerate a whistleblower being subject to retaliation because they wish to raise a concern or have done so.

2. ABOUT THIS PROCEDURE

The School's aims above all to prevent wrongdoing from occurring at any level in the first place. However, should wrongdoing occur, the objective is to address it and prevent it from recurring.

The purpose of this procedure (the "**Procedure**") is therefore to create a culture of openness, transparency and accountability, which is essential in order to create social corporate responsibility and prevent any act or omission that is unlawful or defeats the object or the purpose of European or Luxembourgish legal provisions (a "**Breach**"). This Procedure aims to guarantee a framework in which workers **[and third parties]** can communicate about Breach(es) within the School without fear of retaliation.

The School considers compliance with all legal requirements to be essential to the performance of its activities. As a consequence, the School encourages everyone – regardless of their role in the organisation and in every jurisdiction in which the School operates, as the case may be, – to speak up if they suspect a Breach.

This Procedure guarantees a right to report Breaches – with accompanying safeguards –, however, reporting is not an obligation and it remains optional for everyone.

3. SCOPE OF APPLICATION

3.1 This Procedure applies in the context of professional relationships, to every person who is part of the School's environment:

(a) employees of the School (whether permanent, temporary, full-time or part-time) ("**Staff**");

(b) trainees;

(c) former employees of the School as well as those whose work-based relationship is yet not begun in cases where information on Breaches has been acquired during the recruitment process or other pre-contractual negotiations;

(d) current and former employees of the School's contractors, subcontractors and suppliers and persons involved in pre-contractual negotiations;

(e) volunteers;

(f) current and former self-employed workers in business contact with the School;

(g) corporate governance members (members of the School's administrative, management or supervisory bodies, including non-executive members);

(h) facilitators, i.e. natural persons who assist a whistleblower during the reporting process in a professional context and whose assistance should be confidential;

(i) third parties who are connected with a whistleblower and who are at risk of retaliation in a professional context, such as colleagues or relatives of a whistleblower; and

(j) legal entities belonging to a whistleblower or for which they work, or with which they have a professional relationship.

(the "**Concerned Person(s)**").

3.2 "Breach" does not include work-related personal grievances, which are grievances relating to the current or former employment or engagement of a Staff member or a Concerned Person, which have implications for them personally and do not fall within the definition of "Breach".

Personal work-related grievances may be raised via the Channels of Communication as indicated within the ISL Staff Handbook. Examples of personal work-related grievances include conflicts between Staff members and decisions relating to a Staff member's employment or engagement, such as a transfer, promotion or disciplinary action.

3.3 This Procedure takes account of the Luxembourg law of 16 May 2023 implementing Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (the " **Whistleblowing Law**").

3.4 In the event of a conflict between the provisions of this Procedure, the Whistleblowing Law and any other relevant Luxembourg laws, the provisions of the Whistleblowing Law and any other relevant Luxembourg laws shall prevail.

4. DEFFINITION OF WHISTLEBLOWING

4.1 Speaking up or whistleblowing is the disclosure by a Staff member or a Concerned Person (the "**Whistleblower**") of actual or potential Breaches which have occurred or are very likely to occur in the School, and of attempts to conceal such Breaches.

4.2 This may include:

- criminal activities;
- a health or safety hazard;
- damage to the environment;
- failure to comply with a legal or regulatory obligation;
- bribery or corruption;
- unauthorised disclosure of confidential information;
- conduct that harms or is likely to harm the financial position of the School, its affiliates, branches or subsidiaries directly or indirectly related to the School or its successors;
- conflicts of interest or unlawful taking of an interest; or
- deliberate concealment of any of the above matters.

4.3 Whistleblowers may report Breaches relating to the conduct of School's Staff and third parties, such as suppliers or external service providers, whether based in Luxembourg or elsewhere.

5. RESPONSIBILITY

5.1 The School's duties are to:

- put an internal reporting channel compliant with the Whistleblowing Law and any other relevant Luxembourg laws at the disposal of Staff and Concerned Person(s); and

- protect Whistleblowers against retaliation of any kind.

5.2 Whistleblowers must act in good faith and report genuine information or reasonable suspicions and have reasonable grounds to believe the information on Breaches is true at the time they report it and that it falls within the scope of the Whistleblowing Law.

5.3 Bad faith Whistleblowers will incur sanctions as described in clauses 6.5(c) and 12 of this Procedure.

5.4 Whistleblowers may be held liable if they obtain or access the information reported in a way that constitutes a self-standing criminal offence.

6. PROCEDURE FOR REPORTING INTERNALLY

6.1 General principles

(a) The School encourages Staff and Concerned Persons to report any information or reasonable suspicions obtained in a work-related context regarding actual or potential Breach(es) which have occurred or are very likely to occur, and attempt(s) to conceal such Breach(es) (a "**Report**") via the School's internal reporting channel (an "**Internal Report**"), and before a Report is done via an external channel. This is so that the School can act to prevent harm to Staff and Concerned Persons or to the School's performance or reputation.

(b) The School, with the staff delegation's knowledge, has set up the following procedure for Staff members and Concerned Persons to make an Internal Report through the internal reporting channel. Staff and Concerned Persons should follow the guidelines below to make a Report.

(c) Safeguards are put in place at each stage of the Procedure to prevent the disclosure of any information that could lead to the identification of a Whistleblower. The School's internal reporting channel is designed, implemented and managed in a secure manner that ensures the confidentiality of the identity of the Whistleblower and any third party mentioned in a Report, and prevents unauthorised personnel from accessing it.

(d) In order to ensure optimal operation of this Procedure, particularly Internal Reports, the School has decided to call on an external service provider, namely the law firm:

Arendt & Medernach S.A.

41A Avenue John F. Kennedy

L-1855 Luxembourg

(the "**Service Provider**")

(i) The role of the Service Provider is as follows:

- act as a third party within the meaning of Article 6(4) of the Whistleblowing Law, to which the School's internal reporting channel is outsourced and which is instructed for the purpose of managing Internal Reports. Within this framework, the Service

Provider has appointed a team of three people to receive Reports (the "**Recipients of Internal Reports**");

- assist the School in handling and monitoring Internal Reports; and

- assist the School in carrying out an investigation, as described in clause **Error! Reference source not found.** below (the "**Investigation**"), if the School decides to implement such an Investigation. The Investigation will be carried out by a specialist investigation team.

(ii) Using the services of the Service Provider enables the School to:

- establish and manage the receipt of Reports in a secure manner that guarantees the confidentiality of the identity of the Whistleblower and any third parties mentioned in the Report;

- prevent unauthorised persons from accessing the internal reporting channel;

- ensure that all Internal Reports are dealt with promptly in accordance with the applicable legal provisions;

- prevent potential conflicts of interest and/or internal pressure;

- offer a professional service, provided by experts in the field; and

- ensure that Reports are handled impartially, objectively and confidentially.

(iii) The Service Provider is subject to the same requirements as the School under the Whistleblowing Law. The reporting channel is designed, implemented and managed in a secure manner that guarantees the confidentiality of the identity of the Whistleblower and any third party mentioned in the Report, and prevents access by any unauthorised person.

(iv) The Recipients of Internal Reports will communicate with the School, following receipt of an Internal Report and depending on the circumstances, in order to determine precisely what action should be taken in response to the Internal Report.

6.2 **Internal reporting channel**

The following procedure must be followed by Staff and Concerned Persons wishing to make an Internal Report, as outsourced to the Service Provider:

(a) The Whistleblower should send the Internal Report in writing to the Service Provider as soon as possible after the Breach occurs or the Whistleblower becomes aware of the Breach or potential Breach, using one of the methods below:

(i) **by e-mail**: isl.whistleblowing@arendt.com;

(ii) **by post**: Arendt & Medernach S.A. c/o Whistleblowing Procedures, 41A Avenue John F. Kennedy, L-1855 Luxembourg.

The Report can be made in any of the following languages: French, German, Luxembourgish and English.

One of the Recipients of Internal Reports will record the details of the Internal Report anonymously in a confidential file for monitoring purposes.

(b) The Internal Report should be made in writing and should indicate:

(i) the nature of the Breach;

(ii) the identity of the person(s) concerned;

(iii) the date(s) and time(s) when the Breach was committed or observed;

(iv) the apparent duration of the Breach;

(v) the names of witnesses (if any) to the Breach; and

(vi) the measures already taken (if any) to prevent or stop the Breach.

(c) Where the Whistleblower makes an Internal Report anonymously, such Report may, depending on the circumstances, prevent contact being made with the Whistleblower and thus prevent information being obtained that is necessary and useful to carry out an effective, thorough and efficient investigation on the Breach being reported. Similarly, anonymity may prevent the Whistleblower to be effectively protected against retaliation.

(d) Internal Reports will in principle be investigated as described in clause **Error! Reference source not found.** below (the "**Investigation**") and dealt with promptly in a manner which is consistent with the principle of treating all parties involved with impartiality, fairness and confidentiality, following a fair process, and with due respect for the rights of the Whistleblower and of the alleged perpetrator(s). All Reports will be taken seriously and assessed on their merits and facts.

(e) Where appropriate, the School, after having thoroughly analysed the Internal Report and assessed the overall situation, may decide that such Internal Report is manifestly malicious, false, unfair, unfounded or insignificant and does not require further investigation or follow-up other than sending feedback to the Whistleblower informing them of the closure of the procedure pursuant to clause 6.4(b) of this Procedure.

6.3 Investigation

Whistleblowers do not need to provide evidence or supporting information in order for a Report to be considered valid and thus be further investigated. However, providing the Recipients of Internal Reports (respectively the Authorised Recipient(s) as defined under clause 9.1 below) with supporting evidence will help them to investigate a Report effectively, thoroughly and efficiently, provided that acquiring or accessing such supporting evidence does not constitute a self-standing criminal offence.

If, after an initial analysis of the Internal Report, the School decides to conduct an Investigation, the Investigation will be carried out by a specialised team (the "**Investigators**"), in accordance with the following rules:

(a) If deemed necessary in the course of an Investigation, care will be taken to ensure that the Whistleblower is not placed in a position where they could be identified or subjected to retaliation. Any such action will be taken for the sole purpose of facilitating the Investigation and must not be perceived as prejudicing the outcome of the Investigation, materially altering the Whistleblower's employment contract or as retaliation.

(b) Investigations will always be conducted by unbiased and impartial Investigators who have the necessary experience and knowledge to deal with such matters. The Investigation may be led by the Service Provider.

(c) Notes will be taken during the Investigation.

(d) If the Whistleblower is identified or identifiable, the Investigators will interview the Whistleblower, with their consent, who will be required to give full details of the alleged Breach(es).

(e) The alleged perpetrator(s) of the Breach will be invited to meet with the Investigators, will receive detailed information about the allegations made against them, without prejudice to the confidentiality of the identity of the Whistleblower, and will be given the opportunity to respond to the allegations.

(f) Where witnesses are identified by either party, the Investigators will use their best endeavours to investigate the matter further with such witnesses, without disclosing any information about the identities of the parties involved, to the extent legally possible.

(g) Where an Investigation requires other Staff members or Concerned Persons to be interviewed, the interviews will be conducted in the strictest confidence. The need for confidentiality will be stressed to all Staff members or Concerned Persons involved in the Investigation process and it will be made clear that any breach of confidentiality may result in disciplinary action.

(h) It may be necessary for the Investigators to review correspondence (electronic mailbox or instant messaging system) from the alleged perpetrator and/or any other person following the interview of witnesses. Reviews will be conducted in such a way as to limit the relevant period during which electronic mailbox and/or instant messaging system were exchanged and received to the minimum necessary to verify the allegations made in any Report. The Investigators will screen correspondence by key words before reviewing only the accordingly selected correspondence.

(i) When the Investigation has been completed, a record will be made of the Investigation, its outcome and any action taken, subject to compliance with the GDPR[1] and relevant Luxembourg laws[2] .

6.4 **Timing**

The School recognises that time is of the essence in whistleblowing cases and will therefore abide by the following rules when dealing with whistleblowing investigations:

(a) One of the Recipients of Internal Reports will acknowledge receipt of the Internal Report within seven (7) days from the date of receipt of the Report (the "**Receipt**").

(b) Within three (3) months following the sending of the Receipt or, if no Receipt was sent to the Whistleblower, within three (3) months following the expiry of the period of seven (7) days after the Report was made, the Whistleblower will receive feedback on the action envisaged or taken as follow up, to assess the accuracy of the allegations made in the Internal Report and, where relevant, to address the Breach reported, including through actions such as an internal enquiry, an investigation, prosecution, an action for recovery of funds, or the closure of the procedure and on the grounds for such follow-up (the "**Feedback**").

(c) However, the obligation of confidentiality and/or the fact that the Internal Report was made anonymously may prevent the communication of Feedback to the Whistleblower. The Whistleblower must treat all information provided as part of the Feedback as confidential.

(d) Whilst it is always highly desirable to resolve all Reports at the earliest possible opportunity, this will not always be possible if the investigation is to be both thorough and fair.

(e) The School's Human Resources department is responsible for ensuring the proper follow-up of the Investigation.

6.5 **Outcome**

(a) After the Investigation is concluded, the Investigators and the School will ensure, so far as is reasonably practicable, that the Whistleblower is informed of the overall findings of the Investigation and the action taken or to be taken in accordance with clause 6.4(b).

(b) If a Breach is found to have occurred, this may lead to the School taking disciplinary measures, up to and including dismissal with or without notice.

(c) If it is found that a Report was not made in good faith and was similarly supported (e.g. by witnesses), disciplinary action up to and including dismissal may, if the School deems it appropriate, be taken and the School reserves the right to bring a civil liability action against the bad faith Whistleblower, who will also face fines

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[2] In particular, the law of 1 August 2018 on the protection of individuals with regard to the processing of personal data in criminal and national security matters, as applicable and subject to any future amendments.

ranging from EUR 1,500 to EUR 50,000 and imprisonment ranging from eight (8) days to three (3) months, in accordance with Article 27(5) of the Whistleblowing Law.

(d) If the School fails to comply with its obligations under this Procedure, a Whistleblower may voice its concerns to any external competent authority in accordance with clause **Error! Reference source not found.** of this Procedure.

7. OTHER REPORTING CHANNELS

7.1 Whistleblowers are encouraged to make an Internal Report in accordance with this Procedure to ensure that the Report is handled in the fastest and most efficient manner.

7.2 However, Whistleblowers may report information on breaches using the channels and procedures referred to in Articles 17 and 19 of the Whistleblowing Law, after having first reported through internal reporting channels, or by directly reporting through external reporting channels. In such case, Whistleblowers may report externally to one of the twenty two (22) competent authorities listed on, and in accordance with the procedure described on, the following website **"Lanceurs d'alerte"** (the "**External Report**").

7.3 The Reporting Office ("**Office des signalements**") is the competent body in Luxembourg, should any member of Staff or Concerned Persons require any guidance on how to report a Breach**.**

7.4 In very limited circumstances, Whistleblowers can also make a disclosure of a Breach in the public domain ("Public Disclosure") if:

(a) after an Internal and an External Report or an External Report only, no appropriate action was taken within three (3) months and seven (7) days; or

(b) the Whistleblower has reasonable grounds to believe that:

(i) the Breach may constitute an imminent or manifest danger to the public interest, such as an emergency situation or a risk of irreversible damage; or

(ii) in the case of an External Report, there is a risk of retaliation or there is a low prospect of the Breach being effectively addressed, due to the particular circumstances of the case, such as those where evidence may be concealed or destroyed or where an authority may be in collusion with the Breach perpetrator or involved in the Breach.

Breach(es) disclosed publicly in violation of the Whistleblowing Law summarised in this clause will not give rise to any protection for Whistleblowers, who will incur civil liability for damage suffered by the School].

8. DOCUMENTATION AND DATA PROTECTION

8.1 All relevant documentation, including written statements from Whistleblowers, perpetrators of Breaches and witnesses, meeting minutes and any other relevant supporting documentation, will be kept by the School in accordance with the Whistleblowing Law and for the maximum amount of time provided under relevant Luxembourg laws and GDPR and may be used in the context of disciplinary actions, if any.

8.2 Staff members or Concerned Persons making a Report should endeavour to disclose only information relevant to the Breach and should avoid disclosing client or customer information, personal data related to third parties or other sensitive information that is not relevant to the Breach.

8.3 Where a recording is used for an Internal Report, this will be subject to the consent of the Whistleblower. For oral Reports, the School may record the conversation in a durable and retrievable form or through a complete and accurate transcript of the conversation prepared by the Authorised Recipient(s) with the consent of the Whistleblower. The Whistleblower has the right to check, rectify and agree the transcript of the call by signing it.

8.4 Where a Whistleblower requests a meeting with the Authorised Recipient(s), the School will ensure, subject to the consent of the Whistleblower, that a complete and accurate record of the meeting is kept in a durable and retrievable form. The Whistleblower has the right to check, rectify and agree the transcript of the meeting by signing it.

8.5 Personal data which are clearly not relevant for the processing of a specific Report will not be collected or, if collected accidentally, will be deleted without undue delay.

8.6 Any processing of personal data under the Procedure will be carried out in accordance with the Data Protection Laws (as set out in Annexe 1) and any data protection provisions set out in the data protection policy relating to the protection of whistleblowers attached to the Procedure as Annexe 1 or provided by the Service Provider along with the Receipt (the "**Policy**"). This Policy supplements, to the extent necessary, the School's information notice applicable to the processing of the personal data of the School's employees.

8.7 In relation to legal advice provided to the School by the Service Provider, the Service Provider acts as data controller. In this respect, Staff members or Concerned Persons acknowledge that they have read the Service Provider's information notice attached to the Procedure as Annexe 2 or provided by the Service Provider along with the Receipt.

9. CONFIDENTIALITY

9.1 The information provided by the Whistleblower will be treated as confidential to the extent possible and in accordance with the School's legal obligations and its obligation to conduct a thorough review of the Report. It will be received by the Internal Report Recipients and, where appropriate, shared with the Investigators conducting the Investigation (the Internal Report Recipients and the Investigators are together referred to as the "**Authorised Recipients**") (unless disclosure is prohibited or required by law or by a regulatory authority).

9.2 The identity of the Whistleblower will not be disclosed to anyone other than the Authorised Recipient(s) without the explicit consent of the Whistleblower. This provision also applies to any other information from which the identity of the Whistleblower may be directly or indirectly deduced.

9.3 By way of derogation, the identity of the Whistleblower and any other information mentioned in the Report may be disclosed only if this is a necessary and proportionate obligation imposed by Luxembourg law or European Union law in the context of investigations carried out by national authorities or in the context of legal proceedings, including with a view to safeguarding the rights of defence of the person concerned.

9.4 Disclosures made pursuant to clause 9.3 above shall be subject to appropriate safeguards. In particular, the Whistleblower will be notified before their identity is disclosed, unless such notification is likely to compromise the investigations or legal proceedings concerned.

10. TRAINING

Specific training may be organised for personnel managers to raise their awareness of whistleblowing.

11. PROTECTION OF WHISTLEBLOWERS AND MEASURES AGAINST RETALIATION

11.1 The School will not tolerate any act of retaliation against a Whistleblower because of their Report in accordance with this Procedure and the Whistleblowing Law, objection to a Breach or testimony. Any act of retaliation will be punished by nullifying the act in question.

11.2 To benefit from this protection, the Whistleblower must:

(a) be of good faith, meaning that they had reasonable grounds to believe that the Report was true at the time of reporting, and that the Report fell within the scope of the Whistleblowing Law, and

(b) have made either an Internal Report in accordance with this Procedure, or an External Report or a Public Disclosure in accordance with clause 7.

11.3 Whistleblowers who make an Internal Report, an External Report or a Public Disclosure anonymously, and who are subsequently identified and suffer retaliation, also benefit from the protection provided by the Whistleblowing Law and this Procedure, provided that they meet the conditions in clause 11.2.

11.4 Whistleblowers who make a Report of a European Union Breach to relevant EU institutions, bodies, offices or agencies qualify for protection under the same conditions as persons who make an External Report.

11.5 Retaliation may include, but is not limited to:

- suspension of an employment contract, lay-off, dismissal, failure to renew or early termination of a fixed-term employment contract or equivalent measures;
- demotion or withholding of promotion;
- transfer of duties, change of workplace, reduction in salary, change in working hours;
- withholding of training;
- imposition or administering of any disciplinary measure, reprimand or other penalty, including financial penalties;
- failure to convert a temporary employment contract into a permanent contract, where the employee had legitimate expectations that they would be offered a permanent job;

- coercion, intimidation, harassment or ostracism;
- discrimination, disadvantageous or unfair treatment;
- negative performance assessment or employment reference;
- harm, including to the person's reputation, particularly on social media networks, or financial losses, including loss of business and loss of income;
- blacklisting on the basis of a sector or industry-wide formal or informal agreement, which may entail that the person will not find employment in the future in the sector or industry;
- early termination or cancellation of a contract for goods or services;
- cancellation of a licence or permit;
- psychiatric or medical referrals.

12. DISCIPLINARY MEASURES AND SANCTIONS

12.1 The School may take disciplinary action against perpetrators of Breaches, their accomplices, Authorised Recipients who do not respect their confidentiality obligations in accordance with this Procedure and the Whistleblowing Law, bad faith Whistleblowers and Whistleblowers obtaining or gaining access to information in a criminal way. Depending on the results of the Investigation (if one takes place) and the circumstances, disciplinary measures may be imposed in accordance with the ISL Staff Handbook, the ISL Collective Bargaining Agreement and Luxembourg law and may include but are not limited to:

- negative impact on promotional opportunities;
- exclusion from performance-related bonuses/salary increases;
- formal warning;
- demotion;
- dismissal (with or without notice);
- termination of business relationship; or
- revocation of authority (*ad nutum* revocation).

12.2 The School also reserves the right to impose such other penalty as it considers appropriate based on the circumstances and/or to commence legal proceedings to seek, amongst others, indemnities to compensate for any harm suffered and/or criminal penalties for bad faith Whistleblowers, as described under clause 6.5(c) and/or Whistleblowers who have obtained or accessed information in a manner which constitutes a self-standing criminal offence.

12.3 Any measures taken to stop the Breach will not be to the detriment of the Whistleblower.

12.4 The competent authorities and the *Office des Signalements* may, among other things, impose fines on individuals and legal persons who:

(a) hinder or attempt to hinder a Report;

(b) refuse to or provide false or incomplete information to a competent authority in the context of their investigation;

(c) breach the duty to keep a Whistleblower's identity confidential; or

(d) refuse to remedy an identified Breach.

The fines range from EUR 1,500 to EUR 250,000. These amounts may be doubled in the event of a repeat offence within five (5) years.

12.5 Fines ranging from EUR 1,250 to EUR 25,000 may be imposed on Staff or Concerned Persons who retaliate against Whistleblowers or bring vexatious proceedings against them.

13. LEGAL ACTIONS

13.1 The School reserves the right to refer allegations of Breach to appropriate law enforcement agencies and/or public authorities (including the public prosecutor). Should an investigation lead to a criminal prosecution, it may become necessary for the Whistleblower who reported the Breach to provide evidence or be interviewed by the public authorities. This shall not affect the School's right to investigate and, if appropriate, punish allegations of Breach and vice versa.

13.1 No part of this Procedure prevents a member of Staff or a Concerned Person from:

(a) exercising their legal rights at any time;

(b) initiating communications directly with, cooperating with, providing information to or otherwise assisting in an investigation by any governmental or regulatory body or official or self-regulatory organisation regarding a possible Breach;

(c) making an External Report or a Public Disclosure***.***

14. PROCESS REVIEW

This Procedure will be reviewed regularly and any amendments will be notified to Staff and Concerned Persons.

The School reserves the right to modify this Procedure at any time after involving the staff delegation, if applicable.

15. ANY QUESTIONS?

Any questions relating to this Procedure should be addressed to the **Human Resources Department**.

ANNEXE 1 - DATA PROTECTION POLICY RELATING TO THE PROTECTION OF WHISTLEBLOWERS

All capitalised terms used but not defined in this Annexe have the same meaning ascribed to them in the Procedure.

The purpose of this whistleblower data protection policy (the "**Policy"**) is to provide Staff or Concerned Persons and any other person with information on how their personal data may be processed by the School in the context of the Procedure.

In this regard, the School, acting as data controller, collects, stores and processes, by electronic or other means, personal data provided by Staff or Concerned Persons**,** and any other person (the "**Data Subject(s)**"), in accordance with the provisions of the GDPR and any applicable national data protection law (including, but not limited to, the Luxembourg law of 1 August 2018 organising the National Commission for Data Protection and the general data protection framework, as it may be amended or replaced) (collectively, the "**Data Protection Laws**") and the provisions of this Policy.

Contents

1. WHAT PERSONAL DATA DOES THE SCHOOL COLLECT AND FOR WHAT PURPOSES? 14
2. WITH WHOM WILL PERSONAL DATA BE SHARED? 17
3. WHERE CAN PERSONAL DATA BE TRANSFERRED? 17
4. HOW LONG WILL PERSONAL DATA BE KEPT? 18
5. THE RIGHTS OF DATA SUBJECTS 18
6. IT POLICY 18
7. CHANGES TO THIS POLICY 19

1. WHAT PERSONAL DATA DOES THE SCHOOL COLLECT AND FOR WHAT PURPOSES?

As part of the Procedure, the School may process the following personal data for the following purposes:

1.1 Purpose no. 1: processing and examining Reports

CATEGORIES OF PERSONAL DATA	LEGAL BASES
The School may process the following categories of personal data relating to the Data Subjects: • **Identification details**: name, age, gender, professional title, address; • **Contact details**: e-mail address, telephone number; • **Information on disciplinary matters and grievances**; • **Other information contained in the Report**: statements by the Whistleblower, the alleged perpetrator of the Breach, witnesses etc;	The School uses the following legal bases to process personal data: • **Compliance with a legal obligation** to which the School is subject; • The processing is necessary for the purposes of **carrying out the obligations and exercising the rights specific to the controller or the Data Subject in the field of employment law insofar as** such processing is authorised by European Union law, by the law of a Member State or by a

• **Sensitive data**: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health, data concerning a person's sex life or sexual orientation included in the Report or mentioned by the Whistleblower, the alleged perpetrator or witnesses; • **Personal data relating to criminal convictions and offences**.	collective agreement entered into under the law of a Member State which provides appropriate safeguards for the fundamental rights and interests of the Data Subject;

1.2 **Purpose 2: risk management and establishing, exercising or defending legal claims**

CATEGORIES OF PERSONAL DATA	LEGAL BASES
The School may process the following categories of personal data relating to Data Subjects: • **Identification details**: name, age, gender, professional title, address; • **Contact details**: e-mail address, telephone number; • **Information on disciplinary matters and grievances;** • **Other information contained in the Report**: statements by the Whistleblower, the alleged perpetrator of the Breach, witnesses etc; • **Sensitive data**: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health, data concerning a person's sex life or sexual orientation included in the Report or mentioned by the Whistleblower, the alleged perpetrator or witnesses; • **Personal data relating to criminal convictions and offences.**	The School uses the following legal bases to process personal data: • **The legitimate interests pursued by the School** or by third parties, unless the interests or the fundamental rights and freedoms of the Data Subject require protection of personal data; • Processing is necessary for the **establishment, exercise or defence of legal claims.**

1.3 **Purpose 3: disclosure of information about the identity of the Data Subject or any other information that may directly or indirectly reveal the Data Subject's identity**

CATEGORIES OF PERSONAL DATA	LEGAL BASES
The School may process the following categories of personal data relating to Data Subjects: • **Identification details**: name, age, gender, professional title, address;	The School uses the following legal bases to process personal data: • **The Data Subject's consent.**

• **Contact details**: e-mail address, telephone number; • **Information on disciplinary matters and grievances;** • **Other information contained in the Report**: statements by the Whistleblower, the alleged perpetrator of the Breach, witnesses etc; • **Sensitive data**: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health, data concerning a person's sex life or sexual orientation included in the Report or mentioned by the Whistleblower, the alleged perpetrator or witnesses; • **Personal data relating to criminal convictions and offences.**	

The School may collect personal data from the following sources:

(a) Whistleblowers.

(b) Employees or self-employed persons of the School.

(c) Trainees, interns, apprentices and pupils employed by the School.

(d) The alleged perpetrator(s) of the Breach.

(e) The witness(es).

(f) Members or directors of the School.

(g) Volunteers.

(h) Persons working under the supervision and management of contracting parties, suppliers, and sub-suppliers.

(i) Persons who are reporting information to which they have gained access in a work-related relationship that has ceased since then.

(j) Persons in work-related relationships that have not yet commenced, who report information on violations to which they have gained access during the course of the recruitment process or other pre-contractual negotiations.

(k) The School's legal counsel/Arendt & Medernach S.A.

(l) The service company involved in the investigation/Arendt Regulatory & Consulting S.A.

(m) The School's files and, where applicable, the electronic mailbox or instant messaging system of the alleged perpetrator of the Breach or of other persons in accordance with the provisions of paragraph 6 of this Annexe.

Data Subjects may, at their discretion, refuse to communicate personal data to the School. In this case, the School may not be able to properly process and investigate the Report.

2. WITH WHOM WILL PERSONAL DATA BE SHARED?

The School may communicate the aforementioned personal data to the following entities ("**Recipients**"):

- The Whistleblower/alleged perpetrator of the Breach (as the case may be).
- The School's legal counsel/Arendt & Medernach S.A.
- The service company involved in the investigation/Arendt Regulatory & Consulting S.A.
- External consultants/investigators.
- The police.
- The Public Prosecutor's Office.
- Competent public authorities under the Whistleblowing Law:

The Recipients may, under their own responsibility, disclose personal data to their agents and/or delegates (the "**Sub-Recipients**"), who will process the personal data for the sole purpose of assisting the Recipients in providing their services to the School and/or assisting the Recipients in fulfilling their own legal obligations.

The Recipients and Sub-Recipients may, as the case may be, process personal data as processors (where they process personal data on behalf of and on the instructions of the School and/or the Recipients) or as separate data controllers (where they process personal data for their own purposes, namely the performance of their own legal obligations).

3. WHERE CAN PERSONAL DATA BE TRANSFERRED?

The Recipients and Sub-Recipients may be located either inside or outside the European Economic Area (the "**EEA**") in countries. Where the Recipients and Sub-Recipients are located in a country outside the EEA which benefits from an adequacy decision of the European Commission, the personal data are transferred to the Recipients and Sub-Recipients upon such adequacy decision. Where the Recipients and Sub-Recipients are located outside the EEA in a country which does not ensure an adequate level of protection for personal data or does not benefit from an adequacy decision of the European Commission, the School has entered into legally binding transfer agreements with the relevant Recipients in the form of the European Commission approved model clauses or any other appropriate safeguards pursuant to the GDPR, as well as, if necessary, supplementary measures. In this respect, the Data Subjects have a right to request copies of the relevant document for enabling the personal data transfer(s) towards such countries by writing to the School at the email address: DPO@islux.lu / Data Protection Officer, 36 bd Pierre Dupong, L-1430 Luxembourg, Grand Duchy of Luxembourg.

4. HOW LONG WILL PERSONAL DATA BE KEPT?

The GDPR requires personal data to be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which it is processed.

The School will retain personal data for the duration of the Investigation and for as long as any possible legal action relating to or based on the Report is not time-barred.

In certain circumstances, personal data may be rendered anonymous so that it can no longer be associated with the Data Subjects, in which case it no longer constitutes personal data and may be kept for an unlimited period. When the School no longer needs the personal data for the purposes for which it was collected, it will destroy it securely in accordance with the applicable laws and regulations and its internal policy in this regard.

5. THE RIGHTS OF DATA SUBJECTS

In accordance with the conditions and limitations laid down in the Data Protection Laws, Data Subjects acknowledge their rights to:

- access their personal data;
- correct their personal data if it is inaccurate or incomplete;
- object to the processing of their personal data;
- restrict the use of their personal data;
- require the deletion of their personal data;
- request the portability of their personal data.

Data Subjects also have the right to withdraw their consent at any time, without this affecting the lawfulness of the processing based on consent prior to its withdrawal.

Data Subjects and any other person whose personal data is processed under the Procedure may exercise the above rights by writing to the School at the following address: **DPO@islux.lu** / Data Protection Officer, 36 bd Pierre Dupong, L-1430 Luxembourg, Grand Duchy of Luxembourg.

Data Subjects and any other person whose personal data is processed under the Procedure also acknowledge the existence of their right to lodge a complaint with the *Commission nationale pour la protection des données* (the "**CNPD**") at the following address: 15, Boulevard du Jazz, L-4370 Belvaux, Grand Duchy of Luxembourg; or with any competent data protection supervisory authority in their Member State of residence.

6. IT POLICY

The School may access the professional electronic mailbox and, where applicable, the instant messaging system made available to Staff as part of their work, where evidence that makes the alleged Breach likely emerges from the Investigation through witness accounts and insofar as this is necessary to conduct the Investigation as required by the Whistleblowing Law, and for its legitimate interests as listed above.

This review may cover the entire period during which the alleged Breach took place and, as far as possible, will use key words to select the correspondence to be reviewed. The review will at all times be carried out in strict compliance with applicable privacy protection laws and regulations.

For Staff, reference is made to the policy on use of the School's IT resources.

7. CHANGES TO THIS POLICY

The School reserves the right to update this Policy at any time and will make an updated copy directly available to the Data Subjects. Data Subjects will be notified of any material updates to the Policy.

ANNEXE 2 - INFORMATION NOTICE FROM ARENDT & MEDERNACH S.A.

In accordance with the legal provisions applicable in the Grand Duchy of Luxembourg regarding the protection of personal data and Regulation (EU) No. 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**Data Protection Laws**"), you acknowledge that Arendt & Medernach S.A., acting as data controller, collects, stores and processes, electronically or by any other means, your personal data provided in connection with your request for services and in order to comply with our legal obligations.

If you are a natural person, the data processed includes your name, address, date and place of birth, nationality, profession, contact details, preferred language of communication, bank details and any other personal data contained in your files. If you are a legal entity, the same categories of data may be processed in respect of (i) contact persons within your organisation and (ii) economic beneficiaries of your organisation ("**Personal Data**").

Personal Data is processed in order to process your requests, manage your files, maintain our commercial relationship, and comply with any applicable legal obligations, in particular with regard to combatting money laundering and the financing of terrorism.

You also have the right to:

(i) access your Personal Data;

(ii) request rectification of your Personal Data if it is inaccurate or incomplete;

(iii) restrict the use of your Personal Data;

(iv) object to the processing of your Personal Data;

(v) request the deletion of your Personal Data; and

(vi) exercise your right to the portability of your Personal Data under certain conditions defined in the Laws relating to the protection of personal data.

You also have the right to object to the processing of your Personal Data for marketing purposes.

The above rights may be exercised by sending an e-mail to dpo@arendt.com or by writing to our Data Protection Officer:

Arendt & Medernach
For the attention of: Nathalie Bloch, Data Protection Officer
41A Avenue John F. Kennedy
L-1855 Luxembourg
Grand Duchy of Luxembourg

You also have the right to lodge a complaint with the *Commission nationale pour la protection des données (CNPD)* at the following address: 15, Boulevard du Jazz, L-4370 Belvaux, Luxembourg; or with any competent data protection supervisory authority of your EU Member State of residence.

Personal Data may be transferred to other entities or individuals located inside or outside the European Union (in particular, our related entities (including Arendt Regulatory & Consulting S.A.), independent experts, notaries, bailiffs or foreign lawyers). Personal Data will under no circumstances be transferred

to third parties located in a country outside the European Union which does not guarantee an adequate level of protection unless you have given your prior written consent to such transfer, or unless we have taken specific measures (such as appropriate contractual clauses) to ensure that data protection obligations have been met. To the extent permitted by law, Arendt & Medernach S.A. and/or Arendt Regulatory & Consulting S.A. may also disclose Personal Data to judicial authorities and/or administrative authorities within and outside the European Union. In any event, any transfer of Personal Data will only be carried out in compliance with the strict obligations of professional secrecy applicable in Luxembourg.

Finally, and subject to the legal statute of limitations, Arendt & Medernach S.A. will not retain your Personal Data for longer than is necessary for the purposes for which it is to be processed.