

25 May 2018

**AMERICAN INTERNATIONAL SCHOOL OF BUDAPEST**

---

**DATA PROTECTION POLICY**

---

## CONTENTS

1. General provisions.....	3
2. Types, Legal basis, purpose and notification of data processings and retention periods .....	3
3. Principles and methods of data processing.....	17
4. Transferring personal data.....	18
5. Data Processors .....	19
6. Persons having access to personal data .....	19
7. Storage and safety of personal data.....	21
8. Procedures for a data breach event.....	22
9. Data Protection Officer .....	23
10. Data Protection Impact Assessment.....	24
11. Data disposal .....	24
12. Rights of data subjects.....	25
13. Remedies .....	27
14. Amending the Data Protection policy .....	27
ANNEX 1. Data processors (“ <i>Adatfeldolgozók</i> ”) .....	29
ANNEX 2. Privacy Notes Samples .....	32
ANNEX 3. Rules of the Operation of Surveillance Camera System .....	37
ANNEX 4. REGISTER ON DATA TRANSFERS .....	39
ANNEX 5. Notification Form for the event of Personal Data Breach.....	47
ANNEX 6. INTERPRETATION .....	50
ANNEX 7. SCHEDULE 1 OF THE EMMI DECREE.....	53

## **1. GENERAL PROVISIONS**

### **1.1 Goals and objectives of this Policy**

The American International School of Budapest, hereinafter “**AISB**” or the “**School**”, by the nature of the activities performed, collects and uses certain personal data from individuals who may be parents, students, suppliers, business contacts, employees and other individuals the organization has a relationship with or may need to contact.

This Data Protection Policy (“**Policy**”) describes how personal data is collected, handled and stored to meet the School’s data protection standard and to comply with the General Data Protection Regulation (“**GDPR**”) and the Hungarian Act no. CXII of 2011 on information self-determination and freedom of information (“**Data Protection Act**”) as well as with other relevant legal rules.

The policy aims to provide the general framework for ensuring an adequate level of protection for personal data of students, parents or legal guardians of students, employees, and contractual partners processed by AISB.

### **1.2 Scope**

- (a) This policy applies to all personal data we process regardless of the location where that personal data is stored and regardless of the data subject.
- (b) All staff, volunteers, contractors and other people processing personal data on the School’s behalf must read this Policy. A failure to comply with this Policy may result in disciplinary action.

### **1.3 Interpretation**

- In the present Policy, the expressions with a capital letter are defined in [ANNEX 6](#) of this Policy.

## **2. TYPES, LEGAL BASIS, PURPOSE AND NOTIFICATION OF DATA PROCESSINGS AND RETENTION PERIODS**

The School processes the following Personal Data of:

- Students, including potential applying students (see details in section [2.1](#), [2.2](#));
- Alumni (see details in section [2.3](#));
- Parents of the Students (see details in section [2.4](#));
- Job applicants (see details in section [2.5](#), [2.6](#))
- Teachers (including substitute teachers, assistant teachers, coaches and counsellors and administrators (SLTs)) and other Employees (including administrative staff, security guards and maintenance staff etc.) (see details in section [2.7](#));
- Board members (see details in section [2.9](#))
- External suppliers, including visiting specialists (see details in section [2.10](#));
- Any person visiting the Website (see details in section [2.10](#));

- Any person visiting the School, including guests, relatives of Students, etc. (see details in section 2.11);
- Any person whose image is recorded through surveillance camera (see details in section 2.12);

on the following basis, for the following purposes, applying the following retention periods:

## 2.1 Processing of Personal Data of potential applying Students and their Parents

### 2.1.1 Legal Basis:

- Processing is necessary for the purposes of the legitimate interests pursued by the School (GDPR Article 6, section 1 (f));
- Data Subjects have given their consent to the processing of their Personal Data for one or more specific purposes (GDPR Article 6, section 1 (a));
- Data Subjects have given their explicit consent for the processing of their sensitive data (GDPR Article 9, section 2 (a)).

### 2.1.2 Types of data and purposes of processing:

TYPE OF DATA	PURPOSE OF PROCESSING
<p><b>For potential students: Name, preferred name, gender, date and place of birth; current grade, current and previous schools, languages, address, phone number, citizenship (if not Hungarian, type and number of visa), information provided on the Admission Inquiry Form (if collected from potential student),</b></p> <p><b>For parents: Name, relationship to potential student, gender, e-mail, marital status, address, inquiry information (if collected from parent)</b></p>	<p>Sufficient execution of the application procedure; for applicants whose application were declined, notification on the next possibility of application (2.1.1 (b) - consent)</p>
<p><b>Medical information of potential students among others vaccinations</b></p>	<p>To check that the student is healthy and does not infects others – (2.1.1 (a) - legitimate interest pursued by the School)</p>
<p><b>Health support needs</b></p>	<p>To check whether the School is able to provide the Student the support he/she requires - (2.1.1 (c) – explicit consent)</p>

- Way to ensure proper notification: data privacy note shall be provided in the “*Admissions Inquiry*” and “*Apply now*” tabs on the School’s website. The sample text of such Privacy Note is attached to this Policy as **ANNEX 2-PART 1**.

2.1.3 Retention Period: until consent is withdrawn.

## 2.2 Processing of Personal Data of Students

2.2.1 Legal Basis:

- (a) Processing is necessary for compliance with a legal obligation to which the controller is subject (GDPR Article 6, section 1 (c)), where the legal obligation is prescribed by Article 41 section (4) and section (9) of the Public Education Act;
- (b) Processing is necessary for the purposes of the legitimate interests pursued by the School (GDPR Article 6, section 1 (f));
- (c) Data Subjects have given their consent to the processing of their Personal Data for one or more specific purposes (GDPR Article 6, section 1 (a));
- (d) Data Subjects have given their explicit consent (GDPR Article 9, section 2 (a)).

2.2.2 Types of data and purposes of processing

TYPE OF DATA	PURPOSE OF PROCESSING
<b>Name; date and place of birth; address gender; citizenship (if not Hungarian, type and number of visa); examination results, disciplinary problems, student ID card number</b>	Maintaining the register of Students prescribed by the Public Education Act (2.2.1 (a) - legal obligation)
<b>Grade; email address; extracurricular school activities both in school and after school (e.g. football or other sport, drama, band, science); locker number, enrolment status, languages, report cards, transcript, progress report, MAP result, nickname/alias; passport and/or other ID number (to validate nationality), medical records (including injections, allergies, diabetics etc.), past school records / background, birth certificate copies, Veracross ID number, photo (to support identification and for access cards, to put into the yearbook, etc.); evaluation results; the fact that the Student has siblings (plan for projected enrolment)</b>	Effectively pursuing the educational activities of the School (2.2.1 (b) - legitimate interest)
<b>Sensitive private information such as family and sexual life</b>	If it is necessary for a counselling session and/or voluntarily shared with AISB by the Student (2.2.1 (d) – explicit consent)
<b>Video recordings and streaming of events of the School</b>	Building a coherent social community in the School (2.2.1 (c) – consent)
<b>Images and sound recorded by CCTV system, transportation information of the Student,</b>	see details in 2.12 below

**date and time of entry and leave – captured through a log-in system operated as part of the CCTV system**

2.2.3 Way to ensure proper notification: Students and their Parents are notified in writing on the processing of Student’s Personal Data upon enrolment (Annex 2 of the Enrolment Agreement). Students and Parents are asked in the beginning of every school year to sign the applicable (Elementary, Middle or High School) Handbook, which includes the specific information on data collection to confirm that they have read, understood and accepted such information.

2.2.4 Retention periods:

- (a) Where legal obligation is the basis of processing (2.2.1 (a)): as specified in Article 3, point j) and Article 4 of the Archives Act) and Schedule 1 of the EMMI Decree which is enclosed to this Policy as [ANNEX 7](#);
- (b) Where legitimate interest is the basis of processing (2.2.1 (b)): as long as processing is necessary for the purposes of the legitimate interests pursued by the School except where (i) such interests are overridden by the interests or fundamental rights and freedoms of the Student which require protection of Personal Data or; (ii) if the Student (or the Parent on the Student’s behalf, as applicable) objects the Data Processing and the School cannot justify that its legitimate interest overrides that of the Student;
- (c) Where consent is the legal basis of processing (2.2.1 (c)): until withdrawal of consent (consent can be withdrawn by e-mail to the e-mail address ([directoroffice@aisb.hu](mailto:directoroffice@aisb.hu)) or registered postal mail (H-2094 Nagykovácsi, Nagykovácsi út 12., Hungary) with return of receipt (“*tértivevény*”) to the address of the School;
- (d) Where expressed consent is the legal basis (2.2.1 (d)): such Personal Data is only processed as long as it is necessary for the purpose, provided that explicit consent is not withdrawn earlier.

## **2.3 Processing of Personal Data of Alumni**

2.3.1 Legal Basis:

- (a) Processing is necessary for compliance with a legal obligation to which the controller is subject (GDPR Article 6, section 1 (c)), where the legal obligation is prescribed by Article 3, point j) and Article 4 of the Archives Act;
- (b) Data Subjects have given consent to the processing of their Personal Data for one or more specific purposes (GDPR Article 6, section 1 (a));
- (c) Processing is necessary for the purposes of the legitimate interests pursued by the School (GDPR Article 6, section 1 (f)).

2.3.2 Types of data and purposes of processing

TYPE OF DATA	PURPOSE OF PROCESSING
<b>School results and documents necessary to enrol into higher educational institutions</b>	Ensuring exercising the right of Students to education (2.3.1 (a) – legal obligation)
<b>Name, e-mail address, other information Data Subjects choose to share</b>	Sending notifications about Alumni events and maintaining contact (2.3.2 (b) – consent)
<b>Photos of Alumni displayed in former yearbooks</b>	In case of yearbooks prepared during the period when the Alumni were the Students of the School, the School still keeps their pictures in the books after graduation (2.3.1 (c) – legitimate interest)
<b>Images and sound recorded by CCTV system (if Alumni stay in the School building), date and time of entry and leave of the Campus of AISB – captured through a log-in system operated as part of the CCTV system</b>	see details in 2.12 below

- Way to ensure proper notification: upon graduation, graduating Students are notified of the possibility of entering the alumni association and the necessary processing of their personal data in a Google survey message where the Privacy Note also appears. The text of the Privacy Note is attached to this Policy as **ANNEX 2-PART 2**. In the Privacy Note, besides the option of receiving notifications on Alumni events, graduating Students are also notified of (i) the keeping of certain of their Personal Data perpetually as prescribed by the Archive Act, and (ii) the fact that as automatically erasing their photos from former school yearbooks would cause an unreasonable burden for the School, the School still keeps their photos in such yearbooks after graduation. Graduating Students may provide their consent to the processing of their personal data in respect of the receipt of notifications on alumni events by opting in the checkbox in the Google survey website they receive from the School or by sending an e-mail to the e-mail address ([directoroffice@aisb.hu](mailto:directoroffice@aisb.hu)) / clicking the “I consent” tab in the e-mail.

### 2.3.3 Retention periods:

- Where legal obligation is the basis of processing (2.3.1 (a)): as specified in Article 3, point j) and Article 4 of the Archives Act and Schedule 1 of the EMMI Decree;
- Where consent is the legal basis of processing (2.3.1 (b)): until withdrawal of consent. Consent can be withdrawn by e-mail to the e-mail address ([directoroffice@aisb.hu](mailto:directoroffice@aisb.hu)) or registered postal mail (H-2094 Nagykovácsi, Nagykovácsi út 12., Hungary) with acknowledgment of receipt function;
- Where legitimate interest is the legal basis of processing (2.3.1 (c)): until the Alumni objects to such Data Processing for a rightful reason in a way that it does not mean an unreasonable burden for the School. In case of such objections, the School concludes the “balance of interests assessment” test based on the relevant regulations of the GDPR underlining whether the School’s interest to process the Personal Data

is stronger than the rights and interests of the Alumni concerning the processing and notifies the Alumni concerning the result of the assessment.

## 2.4 Processing of Personal Data of Parents of Students

### 2.4.1 Legal Basis:

- (a) Processing is necessary for compliance with a legal obligation to which the controller is subject (GDPR Article 6, section 1 (c)), where the legal obligation is prescribed by Article 41 section (3) of the Public Education Act;
- (b) Processing is necessary for the purposes of the legitimate interests pursued by the School (GDPR Article 6, section 1 (f));
- (c) Processing is necessary for the performance of a contract to which the Data Subject is party (GDPR Article 6, section 1 (b));
- (d) The Data Subjects have given consent to the processing of their Personal Data for one or more specific purposes (GDPR Article 6, section 1 (a)).

### 2.4.2 Types of data and purposes of processing

TYPE OF DATA	PURPOSE OF PROCESSING
<b>Name, address, phone number, family status</b>	Maintaining the register of Students prescribed by the Public Education Act (legal obligation – 2.4.1 (a))
<b>E-mail address</b>	Contacting the Parents in case of necessity (legitimate interest – 2.4.1 (b))
<b>Gender, job title</b>	For using correct salutation on communications (legitimate interest – 2.4.1 (b))
<b>Name, address, e-mail address, passport number and country of issuance, payment information (for tuition and other fees) of the parents or payer (e.g. employer), fees, amount paid, outstanding amounts, late payment information;</b>	Necessary for billing under the enrolment contract (performance of contract – 2.4.1 (c))
<b>Name of spouse</b>	For making spouses eligible to receive academic and personal information on their child (performance of contract – 2.4.1 (c))
<b>Social Media such as LinkedIn, Facebook, Twitter, Instagram Occupation; video recordings and streaming of events in the School;</b>	Building a coherent social community in the School (consent – 2.4.1 (d))
<b>Images and sounds recorded by CCTV system (if Parents stay in the School building) date and time of entry and leave – captured through a log-in system operated as part of the CCTV system</b>	see details in 2.12 below



2.4.3 Way to ensure proper notification: Parents are notified in writing on the processing of Parents' Personal Data upon enrolment (Schedule 2 of the Enrolment Agreement). Parents are asked in the beginning of every school year to sign the applicable (Elementary, Middle or High School) Handbook which includes the specific information on data collection to confirm that they have read, understood and accepted such information.

2.4.4 Retention period:

- (a) Where legal obligation is the basis of processing (2.4.1 (a)): until the end of the school year, but at latest until the full payment of the tuition fee (or the Student otherwise leaving the School);
- (b) Where legitimate interest is the basis of processing (2.4.1 (b)): as long as processing is necessary for the purposes of the legitimate interests pursued by the School except where (i) such interests are overridden by the interests or fundamental rights and freedoms of the Parent which require protection of Personal Data or (ii) if the Parent objects the Data Processing and the School cannot justify that its legitimate interest overrides that of the Parent;
- (c) Where the performance of the contract is the basis of processing:
  - as long as processing is necessary for the performance of the contract; and
  - another 5 (five) years after the expiry of the contract in order to exercise potential claims (in accordance with Section 6:22 (1) of the Civil Code). In this case, Personal Data are processed on the basis of the legitimate interest of the School to the extent it is necessary for the pursuing of the claim;
- (d) Where consent is the legal basis of processing, until withdrawal of consent (consent can be withdrawn by e-mail ([directoroffice@aisb.hu](mailto:directoroffice@aisb.hu)) or registered postal mail (H-2094 Nagykovácsi, Nagykovácsi út 12, Hungary) with acknowledgment of receipt function.

## 2.5 Processing of Personal Data of Job Applicants

2.5.1 Legal Basis:

- (a) Processing is necessary for the purposes of the legitimate interests pursued by the School (GDPR Article 6, section 1 (f));
- (b) The Data Subjects have given consent to the processing of their Personal Data for one or more specific purposes (GDPR Article 6, section 1 (a)).

2.5.2 Types of data and purposes of processing

TYPE OF PERSONAL DATA	PURPOSE OF PROCESSING
Name, e-mail address, phone number, address, qualification and its proof, references, police check ( <i>erkölcsi bizonyítvány</i> )	Sufficient performance of application process (legitimate interest)

<b>in Hungarian) other data in the CV applicant shared with the School</b>	
<b>Photo</b>	In order to use in school materials (consent)

- 2.5.3 Way to ensure proper notification: data privacy note shall be provided in the “Job Postings” page on the School’s website or in the text of job postings published elsewhere. The sample text of such Privacy Note is attached to this Policy as **ANNEX 2-PART 3**.
- 2.5.4 Retention period: until decision is made on the application (hiring), except if the Personal Data are further handled based on section 2.6 or 2.7 below.

## **2.6 Processing of Personal Data of Job Applicants (non-hired)**

### 2.6.1 Legal Basis:

Data Subjects have given their consent to the processing of their Personal Data for one or more specific purposes (GDPR Article 6, section 1 (a));

### 2.6.2 Types of data and purposes of processing

<b>TYPE OF PERSONAL DATA</b>	<b>PURPOSE OF PROCESSING</b>
<b>CVs and data included therein</b>	Informing the data subject on future job postings

- 2.6.3 Way to ensure proper notification: data privacy note shall be provided in the “Job Postings” site on the School’s website or in the text of job postings published elsewhere. The sample text of such Privacy Note is attached to this Policy as **ANNEX 2-PART 3**.
- 2.6.4 Retention period: until the withdrawal of consent. Consent may be withdrawn by e-mail ([directoroffice@aisb.hu](mailto:directoroffice@aisb.hu)), clicking on the “unsubscribe” button or registered postal mail (H-2094 Nagykovácsi, Nagykovácsi út 12. Hungary) with acknowledgment of receipt function.

## **2.7 Processing of Personal Data of hired Employees (e.g. Administrators, Teachers and Staff Members)**

### 2.7.1 Legal Basis:

- (a) Processing is necessary for compliance with a legal obligation to which the Controller is subject (GDPR Article 6, section 1 (c)), where the legal obligation is prescribed by:
- (i) Government Decree no. 32/1999 (II.26.) (in the case of expatriate Administrators, Teachers and other staff),
  - (ii) Article 44/A and 51 section (4) of the Labour Code, Act no. CL of 2017 on the administration of taxation, annex 1, point 3; Act no. LXXXIII of 1997 on health insurance, Article 79 section 2 and Act LXXX of 1997, Article 46 section 2 (only in the case of Hungarian Employees);

- (b) Processing is necessary for the performance of a contract to which the Employee is party (GDPR Article 6, section 1 (b)); and after the expiry of the contract for the purposes of the legitimate interests pursued by the School (GDPR Article 6, section 1 (f));
- (c) Data Subjects have given consent to the processing of their Personal Data for one or more specific purposes (GDPR Article 6, section 1 (a));
- (d) Data Subjects have given their explicit consent for the processing of their sensitive data (GDPR Article 9, section 2 (a));
- (e) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law, preventive or occupational medicine, the assessment of the working capacity of the employee, medical diagnosis (GDPR Article 9, section 2(b), (h))
- (f) Processing is necessary for the purposes of the legitimate interests pursued by the School (GDPR Article 6, section 1 (f)).

2.7.2 Types of data and purposes of processing

TYPE OF DATA	PURPOSE OF PROCESSING
<b>Name, date and place of birth, gender, qualification data concerning educational background and certificates (i.e. name of university, number of diploma, major, graduation data), address, citizenship (in case of other than Hungarian, type and number of visa, residency permits) tax and/or ID card number</b>	Hiring qualified teachers as prescribed by Government Decree no. 32/1999 (II.26.) in the case of Teachers (legal obligation – 2.7.1 (a))
<b>Name, tax ID, date and place of birth, mother’s maiden name, address, beginning of social insurance relation, end of social insurance relation, working time, social security number, FEOR number, qualification data including educational background, the name of educational institution and number of diploma, period of suspension of social insurance; data necessary to determine health insurance benefits, the type of relationship in case of the existence of a dependent person, gross salary and other benefits (e.g.: cafeteria), overtime, social contributions paid, by the School, social contribution deducted, other deductions, health check up</b>	For taxation, health and social security insurance purposes (legal obligation – 2.7.1 (a) + authorisation for the processing of sensitive data in 2.7.1 (e))
<b>Data necessary to determine health insurance benefits; health check-up, the type of relationship in the case of the existence of a dependent person (family details); information on salary, citizenship, ID code, other information required by the Medical insurer</b>	Personal Data collected for expatriate Teachers to provide health insurance (contractual obligation – 2.7.1. (b) + authorisation for the processing of sensitive data in 2.7.1 (e))

<b>Results of annual health exam</b>	Prescribed by the Labour Code (legal obligation – 2.7.1 (a) + authorisation for the processing of sensitive data in 2.7.1 (e))
<b>Results of police/criminal record checks</b>	Prescribed by the Labour Code (legal obligation – 2.7.1 (a) + authorisation for the processing of sensitive data in 2.7.1 (e))
<b>Name, job title, place of employment, date of commencement and termination of employment, social security number, tax ID number (only in case of Hungarian Employees), employees financial information (i.e. bank account number, pension funds, investments), telephone number, e-mail address, times of access, curriculum vitae (CV), time spent in employment so far, rating data, education certificates and diplomas, visa and other residency permits, previous employment and reason for leaving, references, offer letters, employee’s training courses and personal development, professional certificates, skill inventory, foreign language proficiency, salary and compensation, awards and benefits, debt owed to the employee, employee’s expenses, disciplinary records, performance appraisals, paid leaves and holidays, time sheets, allowances and their entitlements, debt owed to the employee, salary and benefits, overtime, substituting, citizenship, gender, family information for health insurance, photo (for identification and ID cards), teaching schedules, marital status (for residency permits), home of record (where they live and want to travel back after), employee’s electronic correspondence (via School provided e-mail) and telephone communication through School phone, driver or other special licences</b>	Entering into and maintaining labour contract relationships (performance of a contract – 2.7.1 (b))
<b>ID copies (e.g. passports, visas)</b>	Providing assistance to expatriate Teachers to arrange all permits to stay, car purchase, apartment rental, payment of fines etc., as well as providing copies to the Immigration Office and the applicable Hungarian consulate (e.g.: New York consulate) (explicit consent – 2.7.1 (d)).
<b>Passports, identification documents</b>	In order to assist expat Teachers in official procedures (consent – 2.7.1 (c))
<b>Video recordings and streaming of events in the School and photos captured on those events,</b>	Building a coherent social community of Students, Parents

<b>Employee and Board member photos on the website</b>	and Teachers of the School (consent – 2.7.1 (c))
<b>References and evaluation materials</b>	In order to make a better assessment of prospecting and present employees (consent – 2.7.1 (c))
<b>Images and sound recorded by CCTV system, date and time of entry and leave – captured through a log-in system operated as part of the CCTV system</b>	see details in 2.12 below

2.7.3 Way to ensure proper notification: data protection clause in the labour contracts and Privacy Notes also referring to this Policy. By signing the labour contract, Employees declare that they read, understood and accepted the Privacy Note and this Policy. The sample text of such Privacy Note is attached to this Policy as **ANNEX 2-PART 4**.

2.7.4 Retention period:

- (a) Where legal obligation is the basis of processing (2.7.1 (a)): as specified in the EMMI Decree (**ANNEX 7** of this Policy) except for those data which are required to exercise the right of Teachers (excluding expatriate Teachers) and Employees to social insurance services (as specified in Article 3, point j) and Article 4 of the Archives Act) which are kept in perpetuity;
- (b) Where legitimate interest is the basis of processing (2.7.1 (b)): as long as processing is necessary for the purposes of the legitimate interests pursued by the School except where (i) such interests are overridden by the interests or fundamental rights and freedoms of the Employee which require protection of Personal Data or; (ii) if the Employee objects to the Data Processing and the School cannot justify that its legitimate interest overrides that of the Employee;
- (c) Where the performance of the contract is the basis of processing:
  - as long as processing is necessary for the performance of the contract except for documents whose retention period is specified otherwise in the EMMI Decree (**ANNEX 7** of this Policy); and
  - another 3 (three) years after the expiry of the contract in order to exercise potential claims after concluding the performance of the contract (in accordance to Section 286(1) of the Labour Code), except for documents whose retention period is specified otherwise in the EMMI Decree (**ANNEX 7** of this Policy). In this case, Personal Data are processed on the basis of the legitimate interest of the School to the extent it is necessary for the pursuing of the claim;
- (d) Where consent is the legal basis of processing, until withdrawal of consent (consent can be withdrawn by e-mail to the e-mail ([directoroffice@aisb.hu](mailto:directoroffice@aisb.hu)) or registered postal mail (H-2094 Nagykovácsi, Nagykovácsi út 12. Hungary) with acknowledgment of receipt function.

**2.8 Processing of Personal Data of Board Members (including applicants for Board Member positions)**

2.8.1 Legal Basis:

- (a) Processing is necessary for compliance with a legal obligation to which the Controller is subject (GDPR Article 6, section 1 (c)), where the legal obligation is prescribed by Act CLXXV of 2011 on the Freedom of Association, on Public-Benefit Status, and on the Activities of and Support for Civil Society Organizations;
- (b) Processing is necessary for the performance of a contract (in this case, performing Board membership) (GDPR Article 6, section 1 (b)); and after the expiry of the contract for the purposes of the legitimate interests pursued by the School (GDPR Article 6, section 1 (f));
- (c) Data Subjects have given their consent to the processing of their Personal Data for one or more specific purposes (GDPR Article 6, section 1 (a));
- (d) Processing is necessary for the purposes of the legitimate interests pursued by the School (GDPR Article 6, section 1 (f)).

TYPE OF DATA	PURPOSE OF PROCESSING
<b>Name, address, mother’s maiden name</b>	Reporting data of the board members to the registration court (legal obligation - 2.8.1 (a))
<b>Name, address, mother’s maiden name, contact details (i.e. e-mail address, telephone number, skype user name)</b>	Entering into and maintaining Board membership (performance of a contract – 2.8.1 (b), legitimate interest – 2.8.1 (d))
<b>Video recordings, CV and other information shared with the School on voluntary basis</b>	Data are shared during the process in the course of which prospective Board Members are being elected (consent – 2.8.1 (c))
<b>Images and sound recorded by CCTV system (if Board Members stay in the School building), date and time of entry and leave – captured through a log-in system and in the CCTV system</b>	see details in 2.12 below

2.8.2 Way to ensure proper notification: data protection clause in the appointment document of Board Members, also referring to this Policy. By accepting the appointment, Board Members declare that they read, understood and accepted this Policy. The School does not provide a separate Privacy Note to Board Members as the range of their Personal Data controlled by the School is not too significant. The sample text of such Privacy Notification is attached to this Policy as [ANNEX 2-PART 4](#).

2.8.3 Retention period:

- (a) Where legal obligation is the basis of processing (2.8.1 (a)): until the data is registered with the registration court, thereafter, the data becomes public data.

- (b) Where the performance of the contract (in this case, performing Board membership) is the basis of processing:
- as long as processing is necessary for the performance of the contract (performing Board membership); and
  - another 5 (five) years after the expiry of the contract (Board membership) in order to exercise potential claims years after concluding the performance of the contract (in accordance with Section 6:22 (1) of the Civil Code). In this case, Personal Data are processed on the basis of the legitimate interest of the School to the extent it is necessary for the pursuing of the claim.

## 2.9 Processing of Personal Data of External Suppliers (including visiting specialists)

### 2.9.1 Legal Basis:

- (a) Processing is necessary for the performance of a contract to which the Data Subject is party (GDPR Article 6, section 1 (b)) (in case the processed Personal Data belong to the natural person External Supplier);
- (b) Processing is necessary for the purposes of the legitimate interests pursued by the School (GDPR Article 6, section 1 (f)):
- (i) in case the processed Personal Data belong to the natural person representative of the External Supplier; and
  - (ii) after the expiry of the term of the contract.

### 2.9.2 Types of data and purposes of processing

TYPE OF DATA	PURPOSE OF PROCESSING
<b>Name, e-mail address, telephone number of representative (in case of company), bank information for payment, ID card number if a private person, passport number, flight and hotel information (in case of visiting specialists only)</b>	Entering into and maintaining contractual relationships, keeping contact (performance of a contract – 2.8.1 (a), legitimate interest – 2.8.1 (b)(i))  Exercising potential claims after the expiry of the contract (legitimate interest – 2.8.1 (b)(ii))

2.9.3 Way to ensure proper notification: data protection clause in the contracts, also referring to this Policy. By signing the contract, External Suppliers declare that they read, understood and accepted this Policy. The School does not provide a separate Privacy Note to External Suppliers as the range of their Personal Data controlled by the School is not extensive. The rules in relation to the Data Processing are included in the privacy clause of the contract between the School and the External Supplier in which this Policy is also referred to.

2.9.4 Retention period: as long as processing is necessary for the performance of the contract; and another 5 (five) years after the expiry of the contract in order to exercise potential



claims years after concluding the performance of the contract (in accordance with Section 6:22 (1) of the Civil Code).

## 2.10 Processing of Personal Data of any Data Subjects visiting the Website

### 2.10.1 Legal Basis:

- (a) Processing is necessary for the purposes of the legitimate interests pursued by the School (GDPR Article 6, section 1 (f));
- (b) The visitors have given consent to the processing of their Personal Data for one or more specific purposes (GDPR Article 6, section 1 (a)).

### 2.10.2 Types of data and purposes of processing

TYPE OF DATA	PURPOSE OF PROCESSING
<b>IP addresses, browsing history by using cookies</b>	Ensuring the technical operation of the Website, providing better online services (legitimate interests – 2.9.1 (a))
<b>Communication in chatbox</b>	Enabling visitors of the website to get in contact with AISB - 2.9.1 (b)

- Way to ensure proper notification: a cookie note and a Privacy Note in the beginning of the conversation in the chatbox ([ANNEX 2-PART 5](#)) and displaying this Privacy Policy on the Website.

### 2.10.3 Retention period:

- (a) Personal Data carried by the cookies may be retained unless the Data Subject as user of the Website blocks their use in its browser settings, but only as long as the processing of such Personal Data is necessary for the technical operation of the Website;
- (b) Personal Data provided in the chatbox: until withdrawal of consent (deletion request).

## 2.11 Processing of Personal Data of any Data Subjects visiting the School (guests, relatives of Students, coaches, consultants, educators etc.)

### 2.11.1 Legal Basis:

Processing is necessary for the purposes of the legitimate interests pursued by the School and third persons entering the School (GDPR Article 6, section 1 (f)).

### 2.11.2 Types of data and purposes of processing

TYPE OF DATA	PURPOSE OF PROCESSING
<b>Name, security ID card number, purpose of visit or person visited, date and time of visit –</b>	Ensuring safety of persons and property (legitimate interests – 2.10.1)



**captured through a log-in system.**

2.11.3 Way to ensure proper notification: a Privacy Note is displayed on the back of the temporary ID cards visitors get. The text of such Note is attached to this Policy as [ANNEX 2-PART 6](#).

2.11.4 Retention period (in accordance with section 32(2)-(3) of the Security Services Act):

- (a) immediately upon the termination of the authorisation for regular entry (but up to a period of 6 months in respect of non-identification details, e.g. date of entry);
- (b) within 24 hours following the time of exit upon a single entry.

## **2.12 Processing of Personal Data of any Data Subjects through surveillance camera (CCTV) system**

2.11.1 Legal Basis:

Processing is necessary for the purposes of the legitimate interests pursued by the School and persons entering the School (GDPR Article 6, section 1 (f)).

2.12.1 Types of data and purposes of processing

<b>TYPE OF DATA</b>	<b>PURPOSE OF PROCESSING</b>
<b>Video recordings of the Data Subjects with in and outdoor campus coverage (no cameras are placed in classrooms, bathrooms, offices and changing rooms)</b>	Ensuring safety of the Employees, Students and properties of the School (legitimate interest).

2.12.2 Way to ensure proper notification: a Privacy Note is displayed in entrances of places monitored including school buses. The text of such Note is attached to this Policy as [ANNEX 2-PART 7](#).

2.12.3 Retention period (in accordance with section 31(2) of the Security Services Act): 3 (three) business days, and in case of certain valuable property, 30 (thirty) business days, unless the Personal Data are used as evidence in a court proceeding or in any other official proceedings in accordance with section 31(5) of the Security Services Act.

2.12.4 Detailed rules of the operation of the surveillance camera system are to be found in [ANNEX 3](#).

## **3. PRINCIPLES AND METHODS OF DATA PROCESSING**

**3.1** The School is committed to the data protection principles set out by the GDPR, i.e. lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality and accountability. This means that School should have a legitimate

basis for which Personal Data are processed. For example, consent from the Data Subject, or that the processing is necessary for compliance with a legal obligation to which we are subject. It also means that we should inform the Data Subject about the processing in accessible and easy to understand communication.

- 3.2** The School only processes the Personal Data based on the legal basis and for the purposes stipulated above in section 2. The range of Personal Data processed can only be in proportion with the purpose of the processing, its scope cannot go beyond that.
- 3.3** In case of Data Processing activities based on consent, the Data Subject may withdraw his consent any time. This does not affect the lawfulness of processing activities before the withdrawal.
- 3.4** If the legal basis of Data Processing is the legitimate interest of the School, the School has concluded and in the future will conclude the “balance of interests assessment” based on the relevant regulations of the GDPR underlining the School’s interest to process the Personal Data is stronger than the rights and interests of the Data Subject concerning the Data Processing. In case of request, the School provides detailed notification to the Data Subjects on the issues stipulated in this section.
- 3.5** In every case when the School wishes to utilize Personal Data for a purpose different from the original purpose, the School notifies the Data Subject and obtains his prior, expressed consent, also provides an opportunity to refuse such Data Processing.
- 3.6** The Data Subject is responsible for the correct provision of his or her Personal Data.
- 3.7** If the Data Processing is based on consent, Personal Data of Data Subjects below 16 years can be processed with the approval of their Parents.
- 3.8** The School may use the statistically unified form of the data, which does not contain any features making possible to identify or make any connection with the Data Subject, therefore, this use of data is not Data Processing.
- 3.9** The School notifies the Data Subject and all persons for whom the Personal Data was transferred on rectification, restriction, or erasure. There is no need for notification if this does not harm the legal interests of the Data Subject, considering the purpose of the Data Processing.

#### **4. TRANSFERRING PERSONAL DATA**

- 4.1** Personal Data of Students may be transferred to courts, police, prosecutors, local governments, child protection organisations, administrative and national security agencies in accordance with the Public Education Act for the lawful requests of these organisations.
- 4.2** Personal Data may be transferred to third persons in case of official legal and administrative procedures to the necessary extent, to administrative agencies based on the official ruling of the agency, legal rules obligations or with the explicit consent of the Data Subject.

- 4.3** The School keeps a register of Personal Data transfers in order to examine the lawfulness of the transfer and notify the Data Subjects, which is attached to this Policy as **ANNEX 4**.
- 4.4** The School utilises software for educational and administrative purposes and Personal Data of Data Subjects may be hosted in the servers of those service providers. List of Personal Data transferred electronically to these external locations are also attached in **ANNEX 4**. These service providers are not considered Data Processors and therefore not listed in **ANNEX 1**, since they provide their own services and make their own decisions on what types of Personal Data they process for their own purposes, and the School has no control over their activities. Nevertheless, the School chooses these service providers after careful consideration of the risk their Data Processing means for the rights and freedoms of the Data Subjects. In case a Data Subject has concerns on processing his or her Personal Data by these service providers, he or she can consult with the privacy policies of these providers, and in case of further concerns, may contact the School in e-mail ([directoroffice@aisb.hu](mailto:directoroffice@aisb.hu)) or registered postal mail (H-2094 Nagykovácsi, Nagykovácsi út 12., Hungary).

## **5. DATA PROCESSORS**

- 5.1** The School utilises Data Processors for several purposes, whose details are listed in **ANNEX 1**. Transfer to the Data Processors is done without obtaining further consent of the Data Subject. Nevertheless, the School must inform the Data Subject on the fact that a Data Processor has been engaged for Data Processing and the identification details of such Data Processors.
- 5.2** Data Processors do not make their own decisions concerning Data Processing; they solely proceed based on their agreement with and the instruction of the School. The School enters into a data processing agreement with Data Processors, specifying at least the minimum requirements under Article 28(3) of the GDPR.
- 5.3** The School regularly inspects the activities of Data Processors, if circumstances necessitate so.
- 5.4** Data Processors can utilise sub-processors only with the consent of the School.

## **6. PERSONS HAVING ACCESS TO PERSONAL DATA**

- 6.1** The Director is responsible for Data Processing activities of the School in general.
- 6.2** It is ensured by this Policy that only persons who need to know shall have access to Personal Data. In case of unauthorised access, an internal examination is conducted to determine possible sanctions. Based on the seriousness of the case, a criminal complaint is also considered. If the unauthorized access is considered as a Data Breach, the process described in section 8 below is followed.
- 6.3** Employees with access to personal data:

- (a) only access personal data to the extent necessary to serve the applicable legitimate purposes for which AISB processes personal data and to perform their job;
- (b) report of any (possible) incident or issue relating to personal data to their manager or to the Business Manager/Director
- (c) never discuss confidential information in public areas or with individuals who don't have a need to know;
- (d) dispose of sensitive documents properly;
- (e) ensure computing devices are password protected and powered off when not in use for extended periods of time (such as after work, on weekends, during holidays and so on);
- (f) working in departments that handle confidential information should lock and secure all information and equipment when they are away from their desk areas;
- (g) should keep their desk areas organized and keep all confidential information secured and out of view when away from their desks;
- (h) should not share passwords;
- (i) should not store the passwords in plain text;
- (j) should promptly report any suspected breach of security policy that comes to their knowledge;
- (k) consult their direct manager or the Business Manager whenever they have concerns regarding the data privacy.

**6.4** Only the following persons have the right to access the following Personal Data:

TYPE OF PERSONAL DATA	PERSON HAVING ACCESS TO PERSONAL DATA
<b>Personal Data of Teachers and other Employees</b>	SLT, HR officer and assistant to the Director for employment related data, finance office for health insurance and payment related data, THE for travel related data and rental of apartments, GSO and his assistant for residency and other permits, car related issues (purchase, insurance, fines, rentals etc.), IT staff.
<b>Personal Data of Students</b>	Teachers, SLT, members of admission office to the extent it is essential for their work, finance office for payment, IT staff
<b>Medical records</b>	Nurses, doctors, counsellors in case of mental health related data; teachers if they also need to know it (e.g. allergies, diabetes, epilepsy, lactose or gluten syndrome of certain Students), members of admission office to the extent it is essential for their work/enrolment, SLT, IT staff

<b>Personal Data of Parents</b>	Teachers, SLT, members of admission office to the extent it is essential for their work, finance office for payment and collection, IT staff
<b>Personal Data of Alumni</b>	SLT, members of admission office, IT staff
<b>Personal Data of External Suppliers</b>	Only those staff members who are responsible for ordering and concluding the contract, IT staff
<b>Personal Data taken by Surveillance Camera System</b>	Director, Business Manager, Security Manager, Security Supervisor

## **7. STORAGE AND SAFETY OF PERSONAL DATA**

- 7.1** Data storage is the processing operation that consists of keeping personal data collected by AISB in any form (electronic or paper).
- 7.2** Personal Data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- 7.3** Personal Data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- 7.4** Personal Data are stored at AISB for the retention period specified in section 2 above, respectively.
- 7.5** The following Personal Data are stored in paper-based format:
- (a) Employee data, employment contracts, leave forms, reimbursement forms, PD forms, travel forms, records of absence, in and outpayment acknowledgments, student test scores, exam papers, essays, medical records, contract with suppliers
  - (b) Security measures for the printed data:
    - (a) users working in departments that handle confidential information should lock and secure all information and equipment when they are away from their desk areas.
    - (b) access controls are implemented as required, to monitor and restrict access for individuals to areas to which access is required for business purposes. These restrictions are applied as required to AISB employees, including contractors, visitors and other relevant identified third parties;
    - (c) AISB will establish retention or disposal schedules for specific categories of records in order to ensure legal compliance, and also to accomplish other objectives, such as preserving intellectual property and cost management.
- 7.6** The majority of Personal Data are stored in electronic format on internal servers and external locations protected by access restriction utilising usernames, passwords and encryption, different levels of authorization, firewalls, and filters. Personal Data stored electronically includes:

- (a) Student, parent, faculty and staff data (in the Veracross system), payroll data (in Kulssoft system), accounting system (SAP), internal and external student test scores, Data Dashboard, surveillance system information.
- (b) Security measures for the electronic data:
  - (a) user should always lock laptop/desktop when leaving from computer
  - (b) user should not circumvent computer security or gain access to a system for which they have no authorization
  - (c) servers and workstations will be protected by using security software and implementing firewall rules;
  - (d) servers will be located in places specially equipped with access control and environmental controls, inaccessible to unauthorized persons;
  - (e) data must be frequently backed up and these copies must be periodically tested to ensure data recovery;
  - (f) employees must use strong passwords for the computer applications used, in accordance with the domain password configuration rules. Passwords must be kept confidential and changed regularly;
  - (g) the access to IT systems (to Personal Data) will be granted by the IT department according to the “need to know” principle, based on privileges required to perform their duties.

**7.7** Internal servers are as follows:

- (a) AISB Enterprise Security Server - runs all security software at the school. All security data is hosted on this server.
- (b) AISB Servers - run at the school. Data storage and backup for all in-house programs are stored here.

Server room can be accessed only by card or key, limited to technology staff only.

**7.8** External locations where Personal Data is hosted are listed in [ANNEX 4](#).

**8. PROCEDURES FOR A DATA BREACH EVENT**

**8.1** In the case of a Data Breach, the person in charge of reporting Data Breaches notifies:

- (a) the Hungarian National Authority for Data Protection and Freedom (“**NAIH**”), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons (see Recital 75 of the GDPR); and

- (b) the Data Subject, when Data Breach is likely to result in a high risk to the rights and freedoms of natural persons (see Recital 89 of the GDPR),

without undue delay, but at least within 72 hours after having become aware of the Breach.

**8.2** The notification is sent in e-mail, with a subject as follows: „URGENT– PERSONAL DATA BREACH”.

**8.3** The notification contains all relevant information concerning the Data Breach. The person in charge remains available to provide further information and respond to any queries of the Data Subject or the NAIH. The notification form for an event of Data Breach listing the information to be provided under Articles 33-34 of the GDPR is attached to this Policy as [ANNEX 5](#).

**8.4** The School pursues all reasonable efforts to solve the problem as fast as possible.

## **9. DATA PROTECTION OFFICER**

**9.1** As the School is

- (a) not a public authority or body (Article 37(1) (a) of the GDPR),
- (b) its core activities do not consist of processing operations which require regular and systematic monitoring of Data Subjects on a large scale (Article 37(1) (b) of the GDPR), and
- (c) its core activities do not consist of processing on a large scale of special categories of data, nor personal data relating to criminal convictions and offences (Article 37(1) (c) of the GDPR),

the School does not appoint a Data Protection Officer.

**9.2** Under Article 37(1) (a) of the GDPR, if Data Processing is carried out by a public authority or body, a DPO shall be appointed by the Data Controller. The Hungarian translation of this Article of the GDPR, however, provides that “public bodies and other bodies performing public duties” (*közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek* in Hungarian) shall appoint a DPO. Education may be interpreted as public duty.

**9.3** As at the date of implementation date of this Policy, neither the GDPR-related amendments of the Data Protection Act nor guidance of the NAIH in respect of the matter specified in section 9.1 has been released. Therefore, the School is not aware of any specific Hungarian rule under which Article 37(1) (a) of the GDPR should be interpreted differently from the wording of the authentic version. Nevertheless, the School will be constantly monitoring updates to the relevant Hungarian laws and the practice of the NAIH, and if necessary, will appoint a DPO.

**9.4** Concerning Personal Data related queries, Data Subjects may contact ([directoroffice@aisb.hu](mailto:directoroffice@aisb.hu)).

## **10. DATA PROTECTION IMPACT ASSESSMENT**

**10.1** The School does not need to conclude a Data Protection Impact Assessment (“**DPIA**”) for the following reasons:

- (a) According to the GDPR, DPIAs have to be carried out if a type of processing, especially the use of new technologies, is likely to create a high risk to the rights and freedoms of individuals. Opinion no. 43 of the W29 Working Party (“**WP29**”), lists those nine criteria that are “likely to result in a high risk” processing. These criteria include Data Processing concerning vulnerable Data Subjects. Children can be considered as not being able to knowingly and thoughtfully oppose or consent to the processing of their data, and they may fall under the category of vulnerable Data Subjects.
- (b) The WP29 considers that the more criteria are met by the processing, the more likely it is to present a high risk to the rights and freedoms of data subjects, and therefore to require a DPIA. As a rule of thumb, a processing operation meeting less than two criteria may not require a DPIA due to the lower level of risk.
- (c) Although the School processes Personal Data of vulnerable Data Subjects, as most processing of Student’s data are statutory obligations (and not based on consent, like in cases of social media sites targeted to children), and as Parents are carefully notified, no “likely to result in a high risk” processing will be made at the School. Therefore, the School does not need to conduct a DPIA.

**10.2** Under Article 35(4)-(5) of the GDPR, NAIH as local data protection authority will have to establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment. NAIH may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. So far, neither of these lists have been disclosed. Nevertheless, the School will be constantly monitoring updates to guidance disclosed by the NAIH, and if necessary, will conduct DPIA.

## **11. DATA DISPOSAL**

**11.1** The School disposes the Personal Data, without undue delay, but within 3 business days from at the latest, upon:

- (a) receiving a request for deletion / revocation of consent made by the Data Subject (if Data Processing is based on consent);
- (b) the expiration of the retention period; or
- (c) the completion of the purpose of the Data Processing.

**11.2** Electronic data are deleted from the servers where they are placed.

**11.3** Disposable paper-based data are physically destroyed by using shredders.



## **12. RIGHTS OF DATA SUBJECTS**

**12.1** The Data Subjects may exercise their rights listed below by contacting the School via e-mail or registered postal mail with return of receipt under the School's contact details as specified in section 5 above. Queries sent in postal mails are regarded authentic if the sender can clearly be identified. Queries in e-mails are regarded authentic only if they are sent from the e-mail address of the Data Subject, which does not preclude other identifications of the Data Subject by the School.

The School examines the queries of the Data Subjects and makes decisions on such requests communicated in writing towards the affected Data Subject without undue delay.

### **12.2 Right to access**

- (a) The Data Subject has the right to obtain from the School confirmation as to whether or not Personal Data concerning him or her are being processed, and, where that is the case, access to the Personal Data and the following information without undue delay:
  - (i) the purposes of the processing;
  - (ii) the categories of Personal Data concerned;
  - (iii) the recipients or categories of recipient to whom the Personal Data have been or will be disclosed, in particular recipients in Third (non EU) Countries;
  - (iv) where possible, the envisaged period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period;
  - (v) the existence of the right to request from the School rectification or erasure of Personal Data or restriction of processing of Personal Data concerning the data subject or to object to such processing;
  - (vi) the right to lodge a complaint with the NAIH;
- (b) Where Personal Data are transferred to a Third Country, the Data Subject has the right to be informed of the appropriate safeguards relating to the transfer.
- (c) The School provides a copy of the Personal Data undergoing processing. For any further copies requested by the Data Subject, the School charges a reasonable fee based on administrative costs and fulfils the request after the payment of the fee. Where the Data Subject makes the request by electronic means, and unless otherwise requested by the Data Subject, the information shall be provided in a commonly used electronic form.
- (d) The right to obtain a copy may not affect the rights and freedoms of others adversely.

### **12.3 Right to rectification**

The Data Subject has the right to obtain from the School without undue delay the rectification of inaccurate Personal Data concerning him or her. Taking into account the purposes of the processing, the Data Subject has the right to have incomplete Personal Data completed, including by means of providing a supplementary statement.

#### **12.4 Right to erasure (“right to be forgotten”)**

- (a) The Data Subjects have the right to ask for the erasure of his or her Personal Data without undue delay.
- (b) The School has the obligation to erase Personal Data without undue delay where one of the following applies:
  - (i) the Personal Data are no longer necessary for the purposes for which they were collected or processed;
  - (ii) the Data Subject withdraws consent on which the processing is based, and there is no other legal ground for the processing;
  - (iii) the Data Subject objects to the processing and there are no overriding legitimate grounds for the processing;
  - (iv) the Personal Data have been unlawfully processed;
  - (v) the Personal Data have to be erased for compliance with a legal obligation in European Union or Hungarian law.
- (c) Where the School has made the Personal Data public and is obliged to erase the Personal Data, the School takes reasonable steps, including technical measures, to inform controllers which are processing the Personal Data that the Data Subject has requested the erasure by such controllers of any links to, or copy or replication of, those Personal Data.

#### **12.5 Right to object**

- (a) The Data Subject has the right to object at any time against the processing of his or her Personal Data, if such processing is necessary for the purposes of the legitimate interests of the School, including profiling. In case the Data Subject objects, the School can no longer process the Personal Data unless the School demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defense of legal claims.
- (b) At the latest at the time of the first communication with the Data Subject, the right to object is explicitly brought to the attention of the Data Subject, presented clearly and separately from any other information.

#### **12.6 Right to restriction of processing**

- (a) The Data Subjects have the right to obtain from the School restriction of processing where one of the following applies:

- (i) the accuracy of the Personal Data is contested by the Data Subject, for a period enabling the School to verify the accuracy of the Personal Data;
  - (ii) the Data Processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restriction of their use instead;
  - (iii) the School no longer needs the Personal Data for the purposes of the Data Processing, but they are required by the Data Subject for the establishment, exercise or defense of legal claims;
  - (iv) the Data Subject has objected to the Data Processing, pending the verification whether the legitimate grounds of the School override those of the Data Subject.
- (b) Where processing has been restricted, such Personal Data, with the exception of storage, is only processed with the Data Subject's consent or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of Hungary.
- (c) A Data Subject who has obtained restriction of the Data Processing is informed by the School before the restriction of Data Processing is lifted.

### **13. REMEDIES**

**13.1** Any Data Processing related queries can be sent to the e-mail address of the School as specified in section 1.2.3 above.

**13.2** In case the Data Subject has the opinion that their complaints were not handled properly, or they believe that their rights were abused in any way, they have the right to search for remedies at the NAIH. The contact information of the NAIH:

Name in Hungarian	Nemzeti Adatvédelmi és Információszabadság Hatóság
Address	1125 Budapest, Szilágyi Erzsébet fasor 22/c.
Mailing address	1530 Budapest, Pf. 5
Telephone	+36 1 391 1400
Telefax	+36 1 391 1410
E-mail	ugyfelszolgalat@naih.hu
Website	www.naih.hu

**13.3** If Data Subjects believe that their rights were abused, they can initiate a court procedure in front of the regional court. Such procedure can be commenced in front of the regional court according to the address or the temporary residence of the Data Subject according to his choice. Upon request, the School notifies the Data Subject on the possibility of legal remedies.

### **14. AMENDING THE DATA PROTECTION POLICY**

**14.1** The School has the right to amend this Policy any time with its unilateral decision.

**14.2** The Data Subject accepts the amended rules of the Policy by becoming aware of its content. Besides providing the possibility of access for the Data Subjects, there is no need to seek the consent of each Data Subject.

**14.3** The effective date and the version number of this Policy can be found on the cover page.

25th May 2018, Nagykovácsi

Paul Slocombe  
Director

**ANNEX 1.**  
**DATA PROCESSORS (“ADATFELDOLGOZÓK”)**

Function	Physician organising and available for health checks
Name	MED-GYÓGYÍTÓ Kft.
Tax ID number	12759859-1-41
Seat/address	1025 Budapest, Csatárka u. 51
Type of data processing	Medical service provider
Function	Kulcssoft payroll system support
Name	Kulcs-Soft Számítástechnika Nyrt.
Tax ID number	13812203-2-41
Seat/address	1022 Budapest, Törökvész út 30/A.
Type of data processing	Have access to the Kulcssoft payroll system while supporting it
Function	Web purchase system support and development
Name	Dialóg Plusz Számítástechnikai Kft.
Tax ID number	10606494-2-41
Seat/address	1137 Budapest, Katona József u. 14.
Type of data processing	Have access to the webpurchase system and SAP data while supporting purchase system of AISB
Function	Doctor of the School for employees (“üzemorvos”)
Name	Dr. Gedeon Anna
Registration number	45085/1998
Seat/address	1025 Budapest, Vihorlát u 32/A.
Type of data processing	Medical service provider
Function	SAP system support
Name	Intelligence Hungary Kft.
Tax ID number	10960273-2-43
Seat/address	1117 Budapest, Neumann János u. 1. Infopark A épület fsz.
Type of data processing	Have access to SAP system while supporting it
Function	Travel agency
Name	ConnecTicket Travel Agency (Utazási Ügynökség)
Tax ID number	14797213-2-41
Seat/address	1053 Budapest, Szép u. 2.
Type of data processing	Using names, passport numbers, date of travel while organizing trips
Function	Technical assistance for providing cafeteria service
Name	OTP Pénztárszolgáltató Zrt.
Tax ID number	13272346-4-41
Seat/address	1051 Budapest, Mérleg utca 4.
Type of data processing	Using data for preparing OTP SZEP card (name, tax number, amount)
Function	Technical assistance for providing cafeteria service
Name	Erzsébet Utalványforgalmazó Zrt.
Tax ID number	24676744-2-44

Seat/address	1146 Budapest, Hermina út 63., II. emelet
Type of data processing	Using data for preparing ERZSEBET card (name, tax number, amount)
Function	Translator
Name	Országos Fordító és Fordításhitelesítő Iroda Zrt.
Tax ID number	10941908-2-42
Seat/address	1062 Budapest, Bajza u. 52.
Type of data processing	Translation of official documents (birth certificate, marriage certificate, driver license)
Function	Customs assistance for teachers
Name	TNT Express Hungary Kft.
Tax ID number	10376166-2-44
Seat/address	1185 Budapest II. Logisztikai központ - Irodaépület BUD Nemzetközi Repülőtér 283. ép.
Type of data processing	Using name, nationality, address, date and place of birth, passport number for custom office (custom clearance), based on consent
Function	Customs assistance for teachers
Name	Federal Express Corporation Magyarországi Fióktelepe
Tax ID number	22246891-2-13
Seat/address	2220 Vecsés Lőrinci út 59. C. ép. 5.
Type of data processing	Using name, nationality, address, date and place of birth, passport number for custom office (custom clearance), based on consent
Function	Support moving of teachers
Name	Putters International Movers Zrt.
Tax ID number	10813951-2-41
Seat/address	1139 Budapest, Forgách utca 9/b
Type of data processing	Using names, addresses and list of belongings together with the dates of moving, employment certification
Function	Support moving of teachers
Name	Gosselin Mobility Budapest Kft.
Tax ID number	11932989-2-43
Seat/address	1094 Budapest, Liliom utca 1/b
Type of data processing	Using names, addresses and list of belongings together with the dates of moving, employment certification
Function	Support moving of teachers
Name	EuroMove & Relocation Kft.
Tax ID number	12813995-2-43
Seat/address	1116 Budapest, Barázda utca 40.
Type of data processing	Using names, addresses and list of belongings together with the dates of moving, employment certification
Function	Support moving of teachers
Name	Move One Moving Company / Tibor Bíró
Tax ID number	10858134-2-43
Seat/address	1117 Budapest, Neumann János u 1/E, 5th Floor

Type of data processing	Using names, addresses and list of belongings together with the dates of moving, employment certification
Function	Support moving of teachers
Name	AGS Budapest
Tax ID number	10897438-2-43
Seat/address	1116 Budapest, Hunyadi János út 162.
Type of data processing	Using names, addresses and list of belongings together with the dates of moving, employment certification
Function	Support moving of teachers
Name	Santa Fe Relocation Kft.
Tax ID number	10845754-2-43
Seat/address	1211 Budapest, Szállító u. 6
Type of data processing	Using names, addresses and list of belongings together with the dates of moving, employment certification
Function	Making professional photos for the Yearbooks
Name	PRI Kft. (Rónaszéki Péter)
Tax ID number	14905180-2-41
Seat/address	1039 Budapest, Hunyadi u. 38.
Type of data processing	Using name, grades of students e-mail address of parents, position of Faculty and Staff while making the photos and agreeing on the right one
Function	HootBoard- Community Message Board support
Name	HootBoard LLC
Tax ID number	471535857
Seat/address	2 Spring Lane, Yardley, PA 19067, United States
Type of data processing	Supporting AISB's Community Message Board

**ANNEX 2.**  
**PRIVACY NOTES SAMPLES**

**PART 1**  
**PRIVACY NOTE FOR APPLYING STUDENTS**

By providing your Personal Data during the application process, you consent that your Personal Data will be processed by the School for the purposes of the successful execution of the application process. You may find further information and details of such processing in our Data Protection Policy accessible at [[www.aisb.hu](http://www.aisb.hu)].

**PART 2**  
**PRIVACY NOTE FOR ALUMNI ON PROCESSING THEIR PERSONAL DATA AFTER GRADUATION**

We hereby notify you that we keep your Personal Data which are necessary for you in order to move into higher education perpetually as prescribed by law. Also, as automatically erasing your photos from former school yearbooks would cause an unreasonable burden for us, we still keep your photos in such yearbooks after graduation.

You, as a graduate of the School, may provide your consent for AISB in order to contact you in the future and such to the processing of your Personal Data by the School for the purposes of notifying you about alumni events. You may give your consent by sending an e-mail to the e-mail address [alumni@aisb.hu](mailto:alumni@aisb.hu) with acknowledgment of receipt function clicking the “I consent” tab in the e-mail.

Detailed rules on the processing your Personal Data (including your rights and remedies in relation to such processing) are to be found in our Data Protection Policy accessible on [www.aisb.hu](http://www.aisb.hu).

**PART 3**  
**PRIVACY NOTE FOR JOB APPLICANTS**

Applicants

Personal Data you disclose during the application process will be processed by the School for the purposes of the successful execution of the application process. You may find further information and details of such processing in our Data Protection Policy accessible at [[www.aisb.hu](http://www.aisb.hu)].

Declined applicants

Unfortunately we decided not to hire you this time, but if you wish to be informed on our similar vacancies in the future, please provide your consent thereto by and the relating processing of your Personal Data [replying to this e-mail] / [clicking on the consent button]. If you do not intend to receive notifications anymore, you may de-register any time by sending an e-mail to the e-mail



[directoroffice@aisb.hu](mailto:directoroffice@aisb.hu). You may find further information and details of the processing of your Personal Data in our Data Protection Policy accessible at [[www.aisb.hu](http://www.aisb.hu)].

## PART 4

### PRIVACY NOTE FOR TEACHERS OTHER EMPLOYEES, AND BOARD MEMBERS

#### Adatvédelmi tájékoztató

Ez a dokumentum (a továbbiakban: „Tájékoztató”), amely a Faculty Handbook része, a Munkavállaló részére az American International School of Budapest-tel („Munkáltató”) kötött munkaszerződésének kezdetén, ill. ha azt korábban kötötték az Adatvédelmi Szabályzat kidolgozását követően kerül átadásra. A Munkavállalónak a Tájékoztatót el kell olvasnia és meg kell értenie. A munkaszerződése aláírásával a Munkavállaló egyben kijelenti, hogy megértette a Tájékoztató tartalmát. A Tájékoztató az Európai Parlament és a Tanács (EU) 2016/679 számú, a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló rendeletének (általános adatvédelmi rendelet, „**GDPR**”), valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény alapján részletes tájékoztatást tartalmaz a Munkavállaló személyes adatainak Munkáltató által történő kezeléséről az alábbiak szerint:

#### 1. Cél és jogalap

A Munkáltató a Munkavállaló személyes adatait, munkavállalással kapcsolatos célok érdekében kezeli. Ez magában foglalja az adatok felhasználását a munkaszerződés teljesítésére, a jogszabályi követelményeknek való megfelelésre, és a Munkáltató jogos érdekeinek érvényesítésére. A különböző adattípusok tekintetében az adatkezelési célok és jogalapok részletes listája a Munkáltató Adatvédelmi Szabályzatában található.

#### 2. Adattípusok

A Munkáltató által kezelt személyes adatok típusai, többek között, magukban foglalják a Munkáltató [www.aisb.hu](http://www.aisb.hu) oldalon hozzáférhető Adatvédelmi Szabályzatának 2.4. pontjában foglalt adatokat, így többek között, a munkavállaló személyi és kapcsolattartási adatait, bérszámfejtéshez, juttatásokhoz és költségekhez szükséges információt, szabadság, betegszabadság és egyéb távollét nyilvántartását;

#### Data Privacy Note

This document (hereinafter: the “**Note**”) is a part of the Faculty Handbook, which is given to the Employee in the beginning of his/her employment with the American International School of Budapest (the “**Employer**”), or after the implementation of ‘AISB Data Protection Policy. The Note must be read and understood by the Employee. By signing the Employment Agreement, the Employee declares that he acknowledged the content of this Note. The Note contains a detailed notification concerning the processing of the Employee’s personal data by the Employer in accordance with regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR) and Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter referred to as “Information Act”) as follows:

#### 1. Purpose and legal basis

The Employer keeps and processes the Employee’s personal data for employment purposes. This includes using data to comply with the employment contract, to comply with legal requirements, and pursue its legitimate interests. The detailed list of purposes and legal bases for different data types can be found in the Data Protection Policy of the Employer.

#### 2. Types of data

The types of personal data the Employer processes include [the data specified in section 2.4 of the Data Protection Policy of the Employer accessible at [www.aisb.hu](http://www.aisb.hu), amongst others, personal identification and contact details of the Employee, information needed for payroll, benefits and expenses purposes; records of holiday, sickness and other absence; and records relating career history, such as training records,

karriertörténettel kapcsolatos dokumentumokat, képzési adatokat, eredményeket, teljesítmény-felméréseket, az éves orvosi alkalmassági vizsgálat eredményét (megfelelt / nem felelt meg), stb.

### **3. Egészségügyi adatok**

Amennyiben szükséges, a Munkáltató tárolhat a Munkavállalóra vonatkozó egészségügyi adatokat, amelyek magukban foglalhatják a távollét okait, jelentéseket és megjegyzéseket. Ezen adatok kezelésére munkahelyi egészségvédelmi és biztonsági követelményeknek való megfelelés érdekében kerül sor. Ezen adatokra ugyanakkor a Munkáltatónak a jogszabályok által előírt és vállalati táppénz, egészségbiztosítás és életbiztosítás adminisztrációja és kezelése miatt is szüksége van.

### **4. Adatok átadása harmadik személyeknek**

Az alábbiakban említettekén kívül a Munkáltató csak akkor ad át munkavállalói személyes adatokat harmadik személyeknek, ha a Munkáltatót e tekintetben jogi kötelezettség terheli, vagy a Munkáltatónak a Munkavállalóval szemben fennálló szerződéses kötelezettségei teljesítéséhez szükséges, például a Munkáltatónak bérszámfejtő, nyugdíj- vagy egészségbiztosító részére kell átadnia azokat.

### **5. Adatfeldolgozók**

A Munkáltató adatfeldolgozóknak munkavállalói személyes adatokat adhat át a munkaviszonyhoz vagy a vállalkozás üzletmenetéhez kapcsolódó célokból, beleértve a bérszámfejtést és egészségügyi vizsgálatot. Az adatfeldolgozók listáját a Munkáltató Adatvédelmi Szabályzata tartalmazza.

### **6. A személyes adatok tárolása és biztonsága**

A Munkavállaló személyes adatai a munkaviszony ideje alatt kerülnek tárolásra, kivéve azokat az adatokat, amelyek megőrzését törvény írja elő, vagy amelyek megőrzéséhez a Munkavállaló hozzájárult. Az adatok megőrzésével kapcsolatos biztonsági intézkedések a Munkáltató Adatvédelmi Szabályzatában találhatóak.

### **7. A Munkavállaló jogai**

A Munkavállalónak joga van a személyes adataihoz való hozzáféréshez, személyes adatainak helyesbítéséhez vagy azok törléséhez, a személyes adatait érintő adatkezelés korlátozásához, tiltakozhat az adatkezelés. A fenti jogok részletes leírását a Munkáltató Adatvédelmi Szabályzata tartalmazza.

### **8. Hozzájárulás visszavonása**

appraisals, other performance measures and the result of yearly medical health checks (capable / not capable), etc.

### **3. Health related data**

Where necessary, the Employer may keep data relating to the Employee's health, which could include reasons for absence, reports and notes. This data will be used in order to comply with health and safety and occupational health obligations. The Employer will also need this data to administer and manage statutory and company sick pay, or health insurance or life insurance policies.

### **4. Disclosure to third parties**

Other than as mentioned below, the Employer only discloses data of the Employee to third parties if the Employer are legally obliged to do so or where the Employer needs to comply with contractual duties to the Employee, for instance the Employer may need to pass on certain information to an external payroll provider, pension or health insurance schemes.

### **5. Data processors**

The Employer may transfer data about the Employee to data processors for purposes connected with employment or the management of the company's business including payroll and health check purposes. The list of data processors can be found in the Employer's Data Protection Policy.

### **6. Storage and security of personal data**

The Employee's Personal Data is stored for the period of employment except those data the retention of which is required by statutory obligation or the Employee provided his consent to holding it. Security measures concerning keeping the data can be found in the Employer's Data Protection Policy.

### **7. The Employee's rights**

The Employee has the right to request access to and rectification or erasure of his Personal Data, the right to restrict processing, object to processing. The details of such rights can be found in the Employer's Data Protection Policy.

### **8. Withdrawal of consent**

Abban az esetben, ha a Munkavállaló hozzájárulását adta bizonyos személyes adatai kezeléséhez, akkor a Munkavállalónak (bizonyos esetekben) joga van a hozzájárulást bármikor visszavonni, ami azonban nincs kihatással a hozzájárulás visszavonása előtti adatkezelés jogszerűségére.

#### **9. Jogorvoslatok**

A Munkavállalónak joga van panasszal fordulni a Nemzeti Adatvédelmi és Információszabadság Hatósághoz vagy a bírósághoz, abban az esetben, ha úgy véli, hogy a Munkavállaló nem felelt meg a Munkavállaló személyes adatainak a kezeléséhez szükséges releváns jogszabályi követelményeknek.

#### **10. Kapcsolattartó**

Abban az esetben, ha a Munkavállalónak bármely aggálya támad az adata kezelésével kapcsolatban, a Munkavállaló az alábbi e-mail-en keresztül kaphat felvilágosítást: [directoroffice@aisb.hu](mailto:directoroffice@aisb.hu)

#### **11. Adatvédelmi Szabályzat**

További információt a Munkavállaló a Munkáltató [www.aisb.hu](http://www.aisb.hu) oldalon hozzáférhető Adatvédelmi Szabályzatban találhat.

If the Employee has provided consent for the processing of certain of his Personal Data, the Employee has the right (in certain circumstances) to withdraw that consent at any time which will not affect the lawfulness of the processing before the consent was withdrawn.

#### **9. Remedies**

The Employee has the right to lodge a complaint to the Hungarian Data Protection Office or to the court if he believes that the Employer have not complied with the requirements of the relevant legal rules with regard to the Employee's personal data.

#### **10. Contact person**

If the Employee has any concerns as to how his data is processed, the Employee can contact by e-mail: [directoroffice@aisb.hu](mailto:directoroffice@aisb.hu)

#### **11. Data Protection Policy**

For further information, the Employee can consult with the Employer's Data Protection Policy accessible at [www.aisb.hu](http://www.aisb.hu).

### **NOTIFICATION FOR BOARD MEMBERS**

Concerning your membership of the School Board, the School hereby notifies you that it processes your personal data to the necessary extent. The details of such data processing can be found in the School's Privacy policy, Data Protection Policy, available in paper format at the reception or on [www.aisb.hu](http://www.aisb.hu).

### **PART 5 COOKIE NOTE**

In order to provide you a customized service, a small data package ("cookie") is placed on your computer. The purpose of the cookie is to ensure the highest quality of the Website, to provide personalized services, to improve your user experience. You can delete the cookie from your computer or set up your browser to disable cookies. By prohibiting the use of cookies, you acknowledge that, without a cookie, the operation of this site may not be complete.

When providing personalized services, we process the following Personal Data by using cookies: demographics and interest information, habits, preferences (based on your browsing history).

### **CHATBOX NOTE**

By starting a conversation in this chatbox, you consent to the fact that AISB processes your personal data you provide in this chatbox. For more information, please see our Data Protection Policy, available in paper format at the reception or on [www.aisb.hu](http://www.aisb.hu).

**PART 6**  
**PRIVACY NOTE FOR VISITORS**

With your entrance, we process your Personal Data for the purpose of safety of persons and goods. For more information, please see our Data Protection Policy, available in paper format at the reception or on [www.aisb.hu](http://www.aisb.hu).

**PART 7**  
**PRIVACY NOTE ON CAMERA SURVEILLANCE**



This place is under camera surveillance for the purpose of ensuring safe and secure environment for our students and community, security and/or property and valuables. The camera surveillance system is controlled by the American International School of Budapest. Recordings are retained for a period of 3 (three) business days] or [30 (thirty) business days in case financial asset or cash above the value of 5.000.000 HUF (five million HUF) might be in danger. For further information, please see our Data Protection Policy, available on our website, or contact by e-mail: [directoroffice@aisb.hu](mailto:directoroffice@aisb.hu).

**ANNEX 3.**  
**RULES OF THE OPERATION OF SURVEILLANCE CAMERA SYSTEM**

1. A closed-circuit television surveillance camera system is operated at the territory of the School in order to ensure the safety of the Employees, Students and other persons entering School territory and properties of the School. During the operation of the System, Employees, Students and other people entering the School territory are recorded (the “**Recording**”), of which images and sound are Personal Data.
2. The System records digitally and is equipped with a movement detection system. The system records movements detected by the cameras in the surveillance areas and the date, time and location. The cameras function 24 hours a day, 7 days a week. The recording quality, depending on the siting, can enable persons to be identified. The majority of the cameras are fixed. Some cameras have a limited power optical zoom making it possible to zoom in on a location or a person to follow him/her if necessary. The System does not use so-called intelligent technologies, is not connected to other systems, does not use covert surveillance, some of the cameras record sound signals but none of them use ‘speech-enabled surveillance cameras’. No cameras cover locations where persons may expect greater respect for their privacy (e.g. bathroom, changing room, etc.).
3. Personal Data captured by the Recordings are processed for the purposes specified in section 5 below, on the legal basis of the legitimate interests pursued by the School and persons entering the School (GDPR Article 6, section 1 (f)).
4. Personal Data captured by the Recordings are retained for the period of 3 (three) business days or 30 (thirty) business days in case financial asset or cash above the value of 5.000.000 HUF (five million HUF) might be in danger, unless the Personal Data are used as evidence in a court proceeding or in any other official proceedings in accordance with section 31(5) of the Security Services Act.
5. Plans showing the location, purpose of operation, areas on which the camera are directed and plans of the cameras are available, upon request, at the security department.
6. The Recordings may be accessed by the employees of the School with the position of Security Manager, Security Supervisor, Business Manager and Director and if necessary to perform supporting technical services (e.g. operation or maintenance of the System) the Data Processor (as specified in section 7 below), under the supervision and instructions of the School. Name of the persons accessing the recordings and date and purpose of access shall be recorded in separate minutes.
7. Supporting technical services (e.g. operation or maintenance) in respect of the System are carried out by LDSZ Vagyonvédelmi Kft., address: 7632 Pécs, Megyeri u. 119, register number: 02-09-062135) as Data Processor under a separate written agreement.
8. In relation to Personal Data recoded by the System, Data Subjects shall have the applicable rights and remedies specified in this Policy (section 13, 14), whereby the rights of the data subjects may be restricted if that proves necessary to ensure the protection of the data subject or the rights and freedoms of other persons (e.g. if a Data Subject wishes to have access to the Recordings in which

s/he appears, it may be necessary to restrict his/her right of access in the event that another person also appears in the same Recording and that person's consent has not been obtained, in so far as the System does not enable the image of a person to be masked).

**ANNEX 4.**  
**REGISTER ON DATA TRANSFERS**

Name Magyar Államkincstár (Hungarian State Treasury)  
Registered seat 1054 Budapest, Hold u. 4.  
E-mail onyf@onyf.allamkincstar.gov.hu  
Description of transfer Data transfer of the Hungarian students like, name, grade, ID number, KIR number - based on regulation in order to get the state subsidy (“*normatív támogatás*”)

Name Nemzeti Adó- és Vámhivatal (National Tax and Customs Administration)  
Registered seat 1054 Budapest, Széchenyi u. 2.  
Company registration number 15303086-2-51  
E-mail nav\_kozpont@nav.gov.hu  
Description of transfer Transfer of income and family status information, data transfer based on law (personal data)

Name Nemzeti Egészségbiztosítási Alapkezelő (National Health Insurance Fund)  
Registered seat 1139 Budapest, Váci út 73/A.  
Company registration number 15328106-2-41  
E-mail helpdesk@neak.gov.hu  
Description of transfer Transfer of deducted burdens, illnesses, data, transfer based on law (purpose, types of date)

Name Külügyminisztérium (Ministry of Foreign Affairs and Trade)  
Registered seat 1027 Budapest, Bem rkp. 47.  
Company registration number 15311344141  
E-mail konz@mfa.gov.hu  
Description of transfer Data transfer for entry visa (personal data)

Name Bevándorlási és Menekültügyi Hivatal (Immigration and Asylum Office)  
Registered seat 1117 Budapest, Budafoki út 60.  
Company registration number 15722744-2-51  
E-mail migracio@bah.b-m.hu  
Description of transfer Data transfer for residence permit, for address change, for replacement of any official document (personal data)

Name DHL Express Magyarország Szállítmányozó és Szolgáltató Kft.  
Registered seat 1185 Budapest, BUD Nemzetközi Repülőtér repülőtér 302. ép.  
Company registration number 10210798-2-44  
E-mail zoltan.bandli@dhl.com  
Description of transfer Data transfer of name, nationality, address, date and place of birth, passport number for custom office (custom clearance), based on consent

Name Nemzetközi Posta Kicserélő Központ

Registered seat Budapest, Liszt Ferenc Nemzetközi Repülőtér 2. Terminál  
 E-mail customer.service@posta.hu  
 Description of transfer Data transfer of name, nationality, address, date and place of birth,  
 (purpose, types of date) passport number for custom office (custom clearance), based on consent

Name Government Customer Service / City Council Office  
 Registered seat i.e. Budakeszi, Hűvösvölgy, Pilisvörösvár, I., II., V., VI., XII. district  
 E-mail  
 Description of transfer Administration regarding parking fines, Car tax, Parking permit,  
 (purpose, types of date) Registration card, Home address change for EU citizens)

Name Consulates of Hungary in the United States of America  
 Description of transfer Providing ID copies (passports, visas) of expatriate Teachers to the  
 (purpose, types of date) Hungarian consulate when organizing moving/entering to Hungary  
 Guarantees applicable in US-EU Privacy Shield Framework  
 case of transfers to third  
 countries (i.e. non EU  
 countries)

Personal Data hosted on the external servers as listed below:

Application Name	Where is it hosted? - Which country?
Google - Suites	Dublin, Ireland Eemshaven, Netherlands Hamina, Finland St Ghislain, Belgium
Veracross	EU & USA
Adobe - Suites	EU
Weebly	USA
NWEA - MAP TESTS	EU and USA
ERB-CTP	USA
WIDA	USA
LiveStream	USA and EU
Follett Destiny	Follet Server
Seesaw	USA
Survey Gizmo	EU - Germany



ManageBac	USA - EU
EBSCO	USA - EU
HUN tax office Programs (ÁNYK)	HU
Atlas	USA
CEM (Centre for Evaluation & Monitoring)	USA
PSAT/SAT	USA
IB DP - online service	EU
Zearn	USA
FlipGrid	USA
Twitter	Ireland
Facebook	USA, EU
Typingweb	USA
Autodesk - Fusion 3016 - Thinker cad	USA
Overdrive ebooks	USA, EU
Questia school	USA, EU
Newsbank	USA
Britannica School Encyclopedia	USA
Libguides	Ireland on Amazon Web Services
Good Reads	USA
Clever	USA
Amplify	USA
Canva	EU
Jstor	USA and EU
New York Times	USA
BrainPop	USA
Gale Database	USA - UK/EU

Finale	Spain
Kahn Academy	USA
Turnitin	UK
Question Bank	EU
Quizlet	USA
NewsELA	USA
Kulcs soft	EU
ReadWorks	USA
Vernier Logger Lite	USA
WebAssign	USA
Desmos	USA
EASY CBM	USA
Grammarly	USA - UK/EU
Spelling city	USA
RazKids	USA
Bandcamp	USA - UK/EU
Olark	USA
Epic Digital Library	USA
SWivl	USA, EU
HyTek Timing - swimming and track	USA
Socrative	USA
Kognity	Sweden
Easel.ly	USA
Padlet	USA
Piktochart	USA
PhET Simulations	USA

inthinking	UK
Pearson Online	US/UK
ReadTheory	USA
sztaki online dictionary	Hungary
Oxford online dictionary	England
Health and Pension funds program	Hungary
Logger Pro	USA
Membean	USA
Rocketlit	USA
TTRS	USA
Touch type read and spell	USA
UCAS	UK/Europe
Biblionasium	USA
Geogebra	Austria
Prezi	EU
Nessy	USA, UK
Instagram	USA, EU
Pintrest	USA, EU
Pivot Interactives	USA
SendEDU	USA
Mathgames	USA
Khan Academy	US
Parchment	US
Pebble go	US
<a href="http://quill.org">quill.org</a>	USA
Diagnostic Questions (website)	EU

Diigo	USA
iBooks	USA, EU
Translate	EU
Dropbox	USA, EU
Explain Everything	US
ShowMe	US
Skype	USA/EU
K-5 Math - Splashmath	USA
Kids A-Z	USA
Paper by FiftyThree	iPad
Puffin	USA
QR Reader 4.1	USA
Spark Video	USA
Starfall ABCs	USA
Starfall Learn to Read	USA
Weather	USA
Wet Dry Try	USA
Pixie 2	USA
Level It Books	USA
SMART Notebook for iPad	Canada
Book Creator	USA
Green Screen	USA
7 Minutes	EU (Sweden)
Heart Rate Free	USA
PE Games	Canada
Race Splitter	USA

SloPro	USA
SmartMotion	Japan
SpeedClock	Sweden
Video Delay	no server
Audible	US/EU
Auditory Memory	US
Hairy Letters	UK
Hairy Phonics	USA, UK
Phonics Awareness, 1st Grade	USA
Sequencing	USA
Sushi Monster	USA
Blokify	USA
Bloxels Builder	USA
BlueBot	UK
Cubelets	USA
Morphi	USA
Playgrounds	USA
Plotaverse	USA
Switch&Glitch	Finland
Tynker	USA
Animation - do ink	IPAD
Geoboard	iPad
Marble Math Jr	USA
MathBingo	USA
Money Pieces	USA
Monster2	USA

MonsterPhonics	USA
Number Pieces	USA
ChatterKid 1.3	USA
Star Rover	USA

**ANNEX 5.**  
**NOTIFICATION FORM FOR THE EVENT OF PERSONAL DATA BREACH**

**ADATVÉDELMI INCIDENS BEJELENTÉSE**  
**[MINTA]**  
**SÜRGŐS!**

**DATA BREACH REPORT**  
**[SAMPLE]**  
**URGENT!**

**CÍMZETT:**  
**KÜLDŐ:**

**TO:**  
**FROM:**

**Cégnév:**

**Name of company:**

**Küldő személy neve: [...]**

- **e-mail címe: [...]**
- **telefonszáma: [...]**
- **fax-száma: [...]**
- **egyéb: [...]**

**Sender's name: [...]**

- **email address: [...]**
- **telephone: [...]**
- **fax: [...]**
- **other: [...]**

**KÜLDÉS DÁTUMA ÉS IDEJE: [...]**

**SENDING DATE: [...]**

**KÜLDÉS MÓDJA:**

- **e-mailen**
- **faxon**
- **egyéb: [...]**

**FORM OF SENDING:**

- **via email**
- **via fax**
- **other: [...]**

**2. KAPCSOLATTARTÓI ADATOK**

**3. DATA OF CONTACT PERSON**

3.1 Az Iskola neve és címe:

3.2 Name and address of the School:

3.3 Az Iskola kapcsolattartójának neve:

3.4 Name contact person at the School:

3.5 Az előbbi személy elérhetőségei (telefonszám, mobiltelefonszám, email-cím):

3.6 Contact information of the person above (phone number, mobile, email address):

**2. A SZEMÉLYES ADATOK  
MEGSÉRTÉSE VONATKOZÓ  
LEGFONTOSABB ADATOK ("ELSŐ  
RÉSZ")**

**3. THE MOST IMPORTANT DATA  
CONCERNING THE PERSONAL DATA  
BREACH ('FIRST PART')**

3.1 Az Adatvédelmi Incidens bekövetkeztek időpontja, szükség esetén becslés alapján:

3.2 Date of the occurrence of the Data Breach (based on estimation, if necessary):

3.3 Az Adatvédelmi Incidens észlelésének időpontja:

3.4 Date of the detection of the Data Breach:

3.5 A Személyes Adatok megsértésének módja és körülményei:

3.6 Form and circumstances of the Personal Data Breach:

3.7 Az érintett Személyes Adatok jellege és tartalma:

3.8 Type and content of the Personal Data in question:

3.9	Az Iskola által az érintett személyes adatok védelmére alkalmazott vagy alkalmazni tervezett műszaki és szervezeti intézkedések:*	3.10	Technical and organisational measures used or planned by the School to protect the Personal Data in question:*
<b>4. A SZEMÉLYES ADATOK MEGSÉRTÉSE VONATKOZÓ TOVÁBBI ADATOK ("MÁSODIK RÉSZ")</b>		<b>5. ADDITIONAL INFORMATION REGARDING THE PERSONAL DATA BREACH ('SECOND PART')</b>	
5.1	Az Adatvédelmi Incidens összefoglalása, megjelölve az adatok megsértésének fizikai helyét és az érintett adathordozót is:	5.2	Summary of the Data Breach, marking the physical place and the medium of the Data Breach:
5.3	Az Érintettek száma:	5.4	Number of Data Subjects involved:
5.5	A lehetséges következmények és kedvezőtlen hatások ismertetése az Érintettekre nézve**:	5.6	Description of possible consequences and unfavourable effects for Data Subjects**:
5.7	A lehetséges kedvezőtlen hatások enyhítésére az Iskola által alkalmazott műszaki és szervezeti intézkedések:	5.8	Technical and organisational measures used by the School to mitigate the possible unfavourable consequences:
<b>6. HATÁRON ÁTNYÚLÓ VONATKOZÁSOK (HA VANNAK)</b>		<b>7. CROSS-BORDER RELATED ISSUES (IF ANY)</b>	
7.1	Az Érintettek között vannak-e más EU tagállamokban élő érintettek:	7.2	Any of the Data Subjects living in other EU member states:

**Megjegyzések az űrlap kitöltéséhez:**

**\* Megjegyzés a fenti 2.5 ponthoz**

Rendkívül fontos részletes tájékoztatást nyújtani azzal kapcsolatban, hogy a *megfelelő technikai védelmi intézkedéseket végrehajtották-e*, vagy, hogy *ezen intézkedéseket alkalmazták-e a biztonság sérelmével érintett adatok tekintetében*.

**\*\* Megjegyzés a fenti 3.3 ponthoz**

Lényeges körülmény, hogy az Adatvédelmi Incidens, azaz a személyes adatok megsértése várhatóan hátrányosan érinti-e az Érintettek személyes adatait vagy magánéletét. A tekintetben, hogy az Adatvédelmi Incidens várhatóan hátrányosan érinti-e az Érintettek személyes adatainak vagy magánéletének védelmét, különösen az alábbiakat kell figyelembe venni:

- a) az érintett személyes adatok jellegét és tartalmát, különösen akkor, ha azok *pénzügyi információkat, különleges adatokat* (pl. vallási, etnikai, szexuális irányultságra vonatkozó, egészségügyi és hasonló adatok), *helymeghatározási adatokat, internetes naplófájlokat, internetes böngészési*

**Notes for filling the form:**

**\* Note for point 2.5 above**

It is highly important to provide detailed notification regarding *whether the appropriate technical protection measures have been implemented or whether those measures have been applied to the data affected by the Data Security Breach*.

**\*\* Note for point 3.3 above**

It is an important circumstance whether the Data Breach, i.e. the breach of personal data is likely to adversely affect the Data Subjects' personal data or private lives. In regards whether the Data Breach would adversely affect the Data Subjects' personal data or private lives, the following shall be considered in particular:

- a) type and content of the affected personal data, especially if they affect *financial information, sensitive data* (e.g. concerning religious, ethnical, sexual orientation, medical and similar data), *localisation data, internet log files, internet browsing history, electronic mailing data;*



*előzményeket, elektronikus levelezési adatokat érintenek;*

- b) a személyes adatok megsértésének várható következményeit az Érintettre nézve, különösen akkor, ha a személyes adatok megsértése személyes adattal visszaéléshez, testi épség sérelméhez, becsületsértéshez, rágalmazáshoz vagy a jóhírnév sérelméhez vezethet; valamint
  - c) a személyes adatok megsértésének körülményeit, különösen akkor, ha a Büntető Törvénykönyvről szóló 2012. évi C. törvényben szabályozott *tiltott adatszerzés* vagy *információs rendszer vagy adat megsértése*, valamint az *információs rendszer védelmét biztosító technikai intézkedés kijátszása* bűncselekmények gyanúja merül fel, vagy az Iskola tudomással bír arról, hogy az adatokat az adatkezelésre nem jogosult személyek kezelik.
- b) the expected consequences of the personal data breach regarding the Data Subject, especially if the breach of the personal data could result personal data abuse, violation of physical safety, slander, defamation or damage to reputation; and
  - c) the circumstances of the breach of personal data, especially if there is a suspicion of the crimes of *illicit access to data, breach of information system or data, or compromising or defrauding the integrity of the computer protection system or device* regulated in Act C of 2012 on the Criminal Code, or the School has the knowledge that the data is controlled by persons who do not have the right to control the data.

**ANNEX 6.**  
**INTERPRETATION**

1. “**AI SB**” means the American International School of Budapest as data controller
2. “**Alumni**” means the former students of the School;
3. “**Archives Act**” means Act LXVI of 1995 on Public Documents, Public Archives and on the Protection of Private Archives Material.
4. “**Board Members**” means members of the board of trustees (*kuratórium* in Hungarian) of the foundation operating the School.
5. “**Data Controller**” means the person, which determines the purposes and means of the processing of Personal Data. In the use of the present Policy, the Data Controller is the School with the basic information as follows:

Name	<b>American International School of Budapest</b>
Registration number	5747
Seat/address	H-2094 Nagykovácsi, Nagykovácsi út 12., Hungary
Person in charge	Mr Paul Slocombe/Ms Klára Armuth
E-mail address	<a href="mailto:directoroffice@aisb.hu">directoroffice@aisb.hu</a>
Website	<a href="http://www.aisb.hu">www.aisb.hu</a>

6. “**Data Processing**” means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
7. “**Data Processor**” means a person which processes Personal Data on behalf of the Data Controller. The details of the Data Processors currently used by the School are as listed in **Data processors** (“*Adatfeldolgozók*”).
8. “**Data Protection Act**” means Act no. CXII of 2011 on information self-determination and freedom of information.
9. “**Data Security Breach**” or “**Data Breach**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
10. “**Director**” means the Teacher who is responsible for the leadership and the management of the School.

11. “**Education Office**” means “*Oktatási Hivatal*”, the Hungarian governmental agency responsible for registering, supervising and organizing public educational activities (address: H-1055 Budapest, Szalay utca 10-14, mailing address: 1363 Budapest, Pf. 19., e-mail address: info@oh.gov.hu, phone number: (36-1) 374-2100, website: [www.oktatas.hu](http://www.oktatas.hu)).
12. “**EMMI Decree**” means EMMI decree no. 20/2012. (VIII. 31.) on the operation of educational institutions.
13. “**Employee**” means employees employed at the School as Administrator, Teacher or Staff Member.
14. “**External Supplier**” means those persons which provide services to the School on the basis of a mandate agreement.
15. “**Finance Office**” means the staff members of the School who are in charge of invoicing and collecting Tuition and other fees
16. “**GDPR**” means Regulation (EU) 2016/679 (General Data Protection Regulation).
17. “**GSO**” means the General Service Officer of the School
18. “**Handbook**” means Elementary, Middle or High School Handbook or Faculty Handbook, whichever is applicable.
19. “**Labour Code**” means Act no. I. of 2012 on the labour code.
20. “**NAIH**” means the Hungarian National Authority for Data Protection and Freedom of Information (in Hungarian: *Nemzeti Adatvédelmi- és Információszabadság Hatóság*).
21. “**Parent**” means any parents of the Student, including other possible guardians.
22. “**Personal Data**” means any information relating to Data Subject by which the Data Subject can be identified; a Data Subject can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
23. “**Policy**” means the present data protection policy of the School.
24. “**Privacy Note**” means a written text which aims to properly notify the Data Subjects on the processing of their Personal Data including the basis, purpose and retention period of the data as well as the related rights of the Data Subjects.
25. “**Public Education Act**” means Act no. CXC of 2011 on national public education.
26. “**School**” or “**AISB**” means the Data Controller.
27. “**Security Services Act**” means Act CXXXIII of 2005 on Security Services and the Activity of Private Investigators.
28. “**SLT**” means the Senior Leadership Team of the School consisting of the Director, Principals, Directors of Learning and Teaching, Advancement Director, IT Director and Business Manager

29. “**Staff**” or “**Staff Member**” means employees at the School other than Faculty Members, including office staff and security guards.
30. “**Student**” means the students of the School.
31. “**Teacher**” means administrators (SLTs), teachers, coaches, assistant teachers and substitute teachers and counsellors at the School.
32. “**THE**” means the Travel, Housing and Event officer of the School
33. “**Third country**” means country outside of the European Union (non EU)
34. “**Website**” means [www.aisb.hu](http://www.aisb.hu).

In case any term is not defined in this section, it has to be interpreted according to the regulations of the Data Protection Act, the GDPR, the Civil Code, the Public Education Act, the Public Employee Act, the Labour Code, Handbook of AISB and other relevant legal rules.

**ANNEX 7.**  
**SCHEDULE 1 OF THE EMMI DECREE**

Document retention plan for schools

<i>Retention item</i>	<i>Subject matter</i>	<i>Retention period (years)</i>
<i>Management, control and HR matters</i>		
1.	Establishment, reorganisation and development of institution	non disposable
2.	Filing books, document disposal protocols	non disposable
3.	HR, salaries and labour matters	50
4.	Labour protection, fire protection, accident prevention	10
5.	Founder's control	10
6.	Professional supervision	20
7.	Agreements, court and official matters	10
8.	Internal policies	10
9.	Civil defence	10
10.	Work plans, reports, Statistics	5
11.	Complaint matters	5
<i>Educational and teaching matters</i>		
12.	Educational, teaching experiments, innovations	10
13.	Registry sheets, replacement registry sheets, editing logbooks	non disposable
14.	Admission, take-over	20
15.	Student disciplinary and damages matters	5
16.	Logbooks	5
17.	Organisation and operation of student government	5
18.	Qualified educational service	5
19.	Organisation and operation of parents' association	5
20.	Consultant, expert opinions, suggestions and recommendations	5
21.	Organization of practical training	5
22.	Exam Protocols	5
23.	Division of subjects	5
24.	Child and youth protection	3
25.	Students' papers, exams, course closure exams	1
26.	Graduation exam, vocational exam	1
27.	Document on the fulfilment of the Community service	5
<i>Economic matters</i>		
27.	Real estate inventory, management, maintenance, building plans without time limits, layout drawings, occupancy permits	
28.	Social security	50
29.	Inventory, fixed asset inventory, asset register, scrapping	10
30.	Annual budget, budget reports, accounting records	5
31.	Operation of workshop	5
32.	Allowances, benefits of children, pupils, fees	5
33.	Expert opinion of expert committee	20
34.	Budget support documents	5