FIRST STEPS DATA PROTECTION POLICY

1.GENERAL PROVISIONS

Goals and objectives of this Policy

The Budapest British International Academy, hereinafter "FIRST STEPS KG" or the "School", by the nature of the activities performed, collects and uses certain personal data from individuals who such as parents, students, suppliers, business contacts, employees and other individuals the School 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, legal guardians of students, employees, and contractual partners of FIRST STEPS KG.

2. TYPES, LEGAL BASIS, PURPOSE AND NOTIFICATION OF DATA PROCESSINGS

The School processes the following Personal Data of:

- Students, including potential applying students
- Parents of the Students
- Job applicants
- Teachers (including substitute teachers, assistant teachers, coaches and other Employees (including administrative staff, security guards and maintenance staff etc.)
- Governing Board members

Processing of Personal Data of Students

Legal Basis:

- 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;
- 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 Persona Data for one or more specific purposes (GDPR Article 6, section 1 (a));
- Data Subjects have given their explicit consent (GDPR Article 9, section 2 (a)).

Processing of Personal Data of Parents of Students

Legal Basis:

- 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;
- 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));
- 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)).

Processing of Personal Data of Job Applicants

Legal Basis:

- 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 (erkölcsi bizonyítvány sufficient performance of application process (legitimate interest) 183450v1 - 10 - in Hungarian) other data in the CV applicant shared with the School.

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

Legal Basis:

- 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); 183450v1 - 11 –
- 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));
- Data Subjects have given 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));
- 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))

- 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 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 Hiring qualified teachers as prescribed by Government Decree no. 32/1999 (II.26.) in the case of Teachers (legal obligation – 2.7.1 (a)) 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 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 For taxation, health and social security insurance purposes (legal obligation – 2.7.1 (a)

Processing of Personal Data of Governing Board Members

Legal Basis:

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

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. PERSONS HAVING ACCESS TO PERSONAL DATA

The Governing Board is responsible for Data Processing activities of the School in general.

It is ensured by this Policy that only persons who need to know shall have access to Personal Data. In case of unauthorized access, an internal examination is conducted

to determine possible sanctions. Based on the seriousness of the case, a criminal complaint is also considered.

Employees with access to personal data:

- only access personal data to the extent necessary to serve the applicable legitimate purposes for which FIRST STEPS KG processes personal data and to perform their job;
- report any incident or issue relating to personal data to their Principal
- never discuss confidential information in public areas or with individuals who don't have a need to know;
- dispose of sensitive documents properly;
- 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);
- working in departments that handle confidential information should lock and secure all information and equipment when they are away from their desk areas;
- should keep their desk areas organized and keep all confidential information secured and out of view when away from their desks;
- should not share passwords;
- should not store the passwords in plain text;
- should promptly report any suspected breach of security policy that comes to their knowledge;
- consult their direct supervisor / Principal whenever they have concerns

5. STORAGE AND SAFETY OF PERSONAL DATA

Data storage is the processing operation that consists of keeping personal data collected by FIRST STEPS KG in any form (electronic or paper).
Personal Data must be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organizational measures.

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.

Personal Data are stored at FIRST STEPS KG for the retention period specified in section 2 above, respectively.

The following Personal Data are stored in paper-based format:

- Employee data, employment contracts, leave forms, reimbursement forms, travel forms, records of absence, in and out payment acknowledgments, student test scores, medical records, contract with suppliers
- Security measures for the printed data:
- FIRST STEPS KG 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.

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:

- Student, parent, faculty and staff data, payroll data, accounting system, internal and external student test scores, Data Dashboard, surveillance system information.
- Security measures for the electronic data:
    - user should always lock laptop/desktop when leaving from computer
    - user should not circumvent computer security or gain access to a system for which they have no authorization
- servers and workstations will be protected by using security software and

- implementing firewall rules;
- servers will be located in places specially equipped with access control

Concerning Personal Data related queries, Data Subjects may contact:

jonabarbara@firststeps.net

APPENDIX A

GDPR Compliance:

All faculty and teaching assistants are Data Controllers under the GDPR. This means you have a responsibility for keeping personal data safe, and for reporting to your Principal any suspected data breach immediately and in any event without fail within 72 hours of it occurring.

To prevent a data breach, please implement the following practices:

1. Do not leave student or faculty/staff personal data unsecured in your room when you are away from your room. Place it in a cupboard/drawer and preferably one that locks. Personal data includes but is not limited to: student photos, tests, test results, medical information, all external test scores, trip financial/payment details, references, report cards, transcripts, athletic stats, student presentations, student essays/reports where student personal opinions are provided.
2. Secure your computer, make it password protected, and make sure you log out when you leave it unattended. Automatic shutdown is recommended. * Do not store or share passwords. Power off your computer when left for extended times (overnight, weekends, holidays.) If you use your school computer offsite, please do not connect to public wifi. Only use secured networks. Make sure your home internet is secure. Do not store school

information on personal computers.

3. Do not use your cell phone to take pictures of school or student-related activities. Use a school device (e.g. camera, iPad).
4. Do not post to social media anything that is school or student-related without checking you have permission from the student and the Principal.
5. Only use school-authorized mobile storage devices with encryption if you need to transfer information. Delete this information as soon as its use has been fulfilled.
6. Only take hard copies of student information off school premises when necessary (e.g. medical information for field trips). Student work can be taken off the premises (for example for grading) but exercise care not to lose it!
7. Google Drive may be used for professional collaboration. It may also be used between students provided that the settings are such that the Owner settings (on each computer) are set to “Disable options to download, print and copy for commenters and viewers”.
8. Make sure you collect information sent to printers/copiers. Shred/file securely copies not used. All stored information on the printer/copier will be deleted at the end of the school day.
9. Dispose of sensitive personal data properly. Delete files/emails from your inbox and empty the Trash when the information is no longer valid or needed. Shred hard copies.
10. Do not share your copier password or your ID badge with anyone.
11. Do not use the same FIRST STEPS KG internal passwords that you use on your own external Internet sites.
12. Do not discuss student/faculty or staff personal information in public areas or with people who don’t have a need to know.
13. Reference writing: At the moment, confidentiality of references is vague in GDPR. If you are asked to write a reference, assume it is open.
14. Principals will send out a message about which software accounts that process personal student data can be used. If you wish to use software that is not on our current published list of agreed software, please contact the Principal to determine what will be needed prior to using that software.
15. When sending email, do not put personal information in the body of the text. Attach a file that is encrypted. Do not send to multiple people with email

addresses shown in the recipient list (use bcc.) Make sure you are sending it to the right people (addresses!)

Budapest, 2019.

To be revised 2020 or as required


First Steps
by Kid's Kiosk®