Information Security Policy
British International School Gdańsk

in accordance with Regulation 2016/679 of the European Parliament and of the Council (EU) of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation data).

1. Purpose

1. The purpose of this document is to introduce consistent rules for maintaining the security of personal data at British International School PL Sp. z o. o. hereinafter referred to as British International School.
2. Information Security Policy is a superior document for other procedures and regulations in the field of personal data protection adopted at the British International School.
3. Information security management is a concept that includes the principles of managing a data protection system and ways of responding to threats. Ensuring appropriate knowledge of the managers of the British International School and the IT network in the field of emerging new threats and methods of protection is another element of ensuring security. Persons operating systems processing personal data are a security link, the effectiveness of which is also influenced by the provision of reliable information on how to safely use software and hardware.
4. The application of this Information Security Policy should ensure security adequate and proportionate to the results of risk assessment for the processed and stored data and in the IT systems of British International School.
5. The Information Security Policy is also a document defining the tasks of management, employees as well as employees and associates of third parties who, under concluded agreements, have access to protected information. It is to help ensure: confidentiality, integrity, availability and accountability of processed personal data and other identified information assets.

2. Scope of processing

1. The Information Security Policy is applied by persons processing personal data and other protected data, regardless of the form of employment at British International School or the legal form binding British International School with that person. In particular, these may be persons employed under an employment contract, interns, apprentices, volunteers and persons performing tasks on the basis of a civil law contract signed with the British International School, as well as employees and associates of third parties with whom an agreement was concluded under which the above-mentioned persons have access to protected information, including personal data.
2. The Information Security Policy covers all personal data and other information subject to protection, processed in the premises of the British International School, regardless of the form of their processing. The personal data policy applies to:
    a) to data processed in traditional filing systems, in particular files, indexes, books, lists and other record collections,
    b) to data processed in IT systems.

3. For the effective implementation of the Information Security Policy, the Administrator provides:

    a) training in the processing of personal data and how to protect it,
    b) periodic assessment of the risk of threats to datasets,
    c) periodic assessment of the impact on the protection of personal data,
    d) control, monitoring and supervision over the processing of personal data,
    e) monitoring of applied security measures,
    f) the possibility of implementing the guidelines contained in the Legal Codes referred to in art. 40 GDPR,
    g) implementation of appropriate technical and organisational measures to ensure a level of security corresponding to the risk;
    h) the ability to ensure the confidentiality, integrity, availability and resilience of processing systems and services at all times;
    i) the ability to quickly restore the availability and access to personal data in the event of a physical or technical incident;
    j) regular testing, measuring and evaluating the effectiveness of technical and organisational measures to ensure the security of processing.

3. Definitions adopted in the analysis of the legality of personal data processing

1. *Data Administrator* (ADO)- British International School PL Sp. z o.o.;
2. *personal data* - information about an identified or identifiable natural person ("data subject"); an identifiable natural person is a person who can be identified, directly or indirectly, in particular on the basis of an identifier such as name and surname, identification number, location data, online identifier or one or more specific physical, physiological, genetic, mental factors, the economic, cultural or social identity of a natural person;
3. *data availability* - it is understood as a feature that ensures data is made available to an authorized entity when needed for processing;
4. *data integrity* - it is understood as a feature that ensures personal data has not been altered or destroyed in an unauthorized manner;
5. *Data Protection Officer (IOD)* - a person appointed by the data administrator and registered with the Personal Data Protection Office to ensure the correctness of data processed at British International School;
6. *violation* of *information security*- any events or actions, including unintentional ones, that may result in a loss of resources, a reduction in the required level of confidentiality, integrity, information availability or system reliability, as well as deviations from applicable procedures, even if they do not lead to negative consequences for the organisation. Events or actions that may lead to a violation of the rights or freedoms of individuals;
7. *violation of personal data protection* - violation of security leading to accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise processed;
8. *data receiver* - a natural or legal person, public authority, agency or other entity to which personal data is disclosed, whether or not it is a third party. Public authorities that may receive personal data as part of specific proceedings in accordance with generally applicable law, however, are not considered recipients - the processing of such data by these public authorities must comply with the provisions on data protection applicable according to the purposes of processing. The term "third party" is understood as a natural or legal person, public authority, unit or entity other than the data subject, administrator, processor or persons who, under the authority of the Administrator or processor - may process personal

data;

9. *person authorized* to *process personal data* – the person who submitted the declaration to ADO on keeping the processed data confidential and the methods of securing this data, having a personal authorization issued by ADO, specifying the name and surname of the authorized person, the date of granting and expiration and the scope of the authorization to process personal data and an identifier, if the data is processed in an IT system;
10. *processing entity* – a natural or legal person, public authority, unit or other entity, which processes personal data on behalf of the Administrator;
11. processing - operations or a set of operations performed on personal data or sets of personal data in an automated or non-automated manner, such as collecting, recording, organising, ordering, storing, adapting or modifying, downloading, viewing, using, disclosing by sending, disseminating or otherwise making available, alignment or combination, restriction, erasure or destruction;
12. *data confidentiality* - it is understood as a feature that ensures data is not made available to unauthorized entities;
13. *data accountability* - it is understood as a feature that ensures, the actions of the subject can be assigned in an unambiguous way only to that entity,
14. *GDPR* - Regulation 2016/679 of the European Parliament and of the Council (EU) of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);
15. *data deletion* - permanent destruction of personal data or its modification in such a way that it will not be possible to determine the identity of the data subject;
16. *authentication* - this is understood as an action aimed at verifying the declared identity of the entity;
17. *user/employee (including* a third *party*) - a person processing data in the system and outside it (e.g. documentation in a traditional form), regardless of the form of employment at the British International School or the legal form binding with this person. In particular, they may be persons employed under an employment contract, interns, apprentices, persons performing tasks on the basis of a signed civil law contract;
18. *data set* - an ordered set of personal data available according to specific criteria, regardless of whether this set is centralized, decentralized or functionally or geographically dispersed;
19. *consent* to *the processing of personal data* - a declaration of will of the person whose data is processed by the data administrator, in which the person expresses approval for this process;

4. Obligations of persons processing personal data

1. Each person processing personal data for the needs of the British International School is obliged to read the content of the Security Policy and strictly comply with its provisions. Persons processing personal data do so on the basis of an authorization issued by the Data Administrator.
2. Employees/users are obliged to comply with generally applicable laws and internal regulations regarding the protection of personal data. To this end, they are obliged to:
    a) apply in writing for the registration of new personal data sets in the list kept by the Data Protection Officer,
    b) ongoing assessment of the functioning of security and protection mechanisms,
    c) submit requests for the introduction of necessary changes in the protection of personal data.

3. If the provisions of separate acts that relate to the processing of personal data provide for more- reaching protection than provided for in the GDPR or the Act, the provisions of these acts shall apply.
4. Employees/users processing personal data are obliged to exercise due diligence in order to protect the interests of persons whose data is collected and processed, and in particular it is necessary to ensure that these data are:
    a) processed in accordance with generally applicable law and internal regulations
    b) collected for specified, lawful purposes and not subjected to further processing inconsistent with these purposes,
    c) factually correct and adequate in relation to the purposes for which they are processed,
    d) stored in a form that allows the identification of data subjects for no longer than it is necessary to achieve the purpose of processing,
    e) and that the information obligation is fulfilled in cases specified in the provisions of generally applicable law.

5. Violation of the provisions of the Information Security Policy may result in blocking the employee's/user's access to protected information and systems. In the event of serious violations, such action may lead to disciplinary action and notice or termination of the contract. In the event of loss as a result of a violation, British International School may pursue legal action for damages.

6. Any violation of information security should be immediately reported to the Administrator and the Data Protection Officer.

7. In the event of detecting a violation of information protection, each employee is obliged to follow the procedures contained in this documentation.

8. Persons responsible for human resources management at the British International School shall immediately inform the IOD or the Data Administrator of any change in the scope of employees' activities that involves a change in the scope of authorization to process protected information.

9. Withdrawal of authorizations to process protected information should take place immediately after the completion of the employee's/user's duties.

5. Areas of personal data processing

1. At the British International School, personal data is processed as part of personal data sets, and the areas of possible personal data processing are: Headmaster's and Deputy Headmaster's office, School office, Classrooms, Teachers' rooms, Library, Computer room, SEN rooms, IT room, Nurse's office.
2. Persons authorized to process personal data may do it only in places designated for this purpose, while maintaining equipment and any other devices dedicated to this activity, with an exception to the procedures described in the Procedure for information security and protection of personal data while working outside the BIS Sp. z o. o.
3. Moving personal data sets outside the processing area is possible with the sole consent of the Data Administrator.

6. Characteristics of personal data sets

1. The personal data sets kept at the British International School are: Employee Data, Employee Recruitment,

Students/Class Participants, Correspondence, Contractor Data, Customer Data and Monitoring.

2. The processing of personal data, in accordance with the purpose of the activity, is possible if it is necessary to fulfill the legitimate interests of the Administrator, and the processing does not violate the rights and freedoms of the data subject. Processing is also allowed when the data subject consents to it, unless it concerns the deletion of data concerning him or it is necessary for the performance of a contract, when the data subject is a party to it, or when it is necessary to take activities before concluding a contract at the request of the data subject. In particular, personal data may be processed when it is necessary to exercise a right or fulfill an obligation resulting from a legal provision, as well as when it is necessary to perform tasks set out by law for the public good.
3. Persons processing the collected data are obliged in particular to:
   a) data processing in accordance with acts of generally applicable law or acts of internal law, to the extent consistent with the authorization signed by the Administrator;
   b) modifying and deleting data, in accordance with the request submitted by the data subject and limiting data processing.