INTERNAL REGULATION – PERSONAL DATA PROTECTION DIRECTIVE

DEFINITION OF TERMS Controller: Blavicon z. s., with its registered office at Pod Holečkovými sady 383/1, 390 01 Tábor, ID: 23322403. **Data Protection Officer (DPO)**: A data protection officer with whom the association (controller) cooperates based on the GDPR regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)). Terms related to personal data issues are defined identically with the GDPR regulation.

1. SCOPE 1.1 This directive regulates the procedures and obligations of the controller, its members, employees, associates, and other persons in handling personal data (hereinafter also referred to as "responsible persons"), the rules for obtaining, collecting, storing, using, disseminating, and retaining personal data. 1.2 This directive is binding for all responsible persons. The directive is also binding for other persons who have another legal relationship with the association and who have committed to act in accordance with this directive.

2. PRINCIPLES OF PERSONAL DATA HANDLING When handling personal data, the controller and responsible persons are guided by the following principles: a) act in handling personal data in accordance with legal regulations, b) handle personal data prudently, not overuse consent to personal data processing, c) process personal data for a specified purpose and within a specified scope and ensure that they are true and accurate, d) process personal data in accordance with the principle of legality – based on legal regulations, in performance of a contract, in performance of a legal obligation of the controller, in protection of vital interests of the data subject or another natural person, in protection of legitimate interests of the controller, in protection of public interest, and personal data processing based on consent, e) respect the rights of the individual who is the data subject, especially the right to grant and withdraw consent to processing, the right to erasure, to object to the scope of processing, etc., f) provide special protection for sensitive data when processing personal data, g) provide information about personal data processing, h) when concluding contracts and legal acts, proceed with regard to the obligation to protect personal data from misuse, i) cooperate with the data protection officer.

3. PROCEDURES OF THE CONTROLLER AND OTHER RESPONSIBLE PERSONS IN HANDLING PERSONAL DATA 3.1 The controller protects all personal data it handles and processes with appropriate and available means against misuse. In doing so, the controller primarily stores personal data in premises, places, environments, or systems to which access is restricted, predetermined, and at all times known to at least the statutory representative of the controller; other persons may gain access to personal data only with the consent of the statutory representative of the controller. 3.2 The controller shall implement measures to ensure that at least the controller's DPO or a person authorized by him/her has an overview of the handling and processing of personal data. These measures include, for example, oral or written information, written communication, establishing obligations in an employment contract, a work performance agreement, a work activity agreement, or a contract concluded by the controller with a third party (e.g., lease agreement, contract for work, service provision agreement). 3.3 The controller shall assess the procedures for handling and processing personal data at least once a year, in the form of a continuous audit. If it is found that some of the controller's procedures are outdated, unnecessary, or have not proven effective, the controller shall promptly take corrective action. 3.4 Each responsible person, when handling personal data, respects their nature, i.e., that they are part of a person's privacy as a data subject, and adapts the associated actions accordingly. The responsible person, in particular, does not publish personal data without verifying that such a procedure is possible, and does not make personal data accessible to persons who do not demonstrate the right to handle them. If such an obligation arises from other documents, the responsible person shall inform

the data subject of their personal data protection rights; or refer them to the chairman of the controller or to the DPO. 3.5 The controller actively cooperates with the data protection officer in handling and processing personal data. The DPO's obligations arise from the GDPR regulation and, where applicable, from the contract concluded with the DPO. 3.6 The controller immediately addresses every security incident concerning personal data, in cooperation with the DPO. If it is likely that the incident will result in a high risk to the rights and freedoms of natural persons, the controller shall always inform that person and communicate what corrective measures have been taken.

4. ORGANIZATIONAL MEASURES FOR PERSONAL DATA PROTECTION IN THE SCHOOL 4.1 All documents containing personal data are permanently stored in lockable cabinets or premises (e.g., in the office) of responsible persons. Other persons may borrow them for the necessary duration to perform activities for the specified purpose. These documents may not be taken out of the controller's premises, handed over to third parties, or copied and copies provided to unauthorized persons. 4.2 All electronic documents containing personal data are always maintained/stored in a secured information system (e.g., Windows operating system). Responsible persons have access to all information systems only based on a login name and password and only within the scope of authorization given by their functional classification (hereinafter referred to as "authorized persons"). When working with the information system, authorized persons must not leave the computer without logging out, may not allow any other person to view it, and must protect the secrecy of the login password; and in case of danger of its disclosure, change it immediately (in cooperation with the network administrator). Accesses are set by the chairman of the controller, who sets the necessary data and computer network security. 4.3 Documents sent outside the controller's premises, e.g., for tax proceedings, judicial proceedings, administrative proceedings, are processed by responsible persons within their duties and powers. These documents must always be transported carefully to prevent unauthorized access to personal data during their handling (e.g., properly sealed when sent by mail). 4.4 In the controller's promotional materials, annual report, on the website, or in other publicly accessible places, personal data may be published to the agreed extent after agreement with the affected persons.

5. CONSENT TO PERSONAL DATA PROCESSING 5.1 For the processing of personal data beyond the scope resulting from laws (or other reasons stipulated by legislation), the consent of the person whose personal data is concerned is necessary. Consent must be informed and specific, preferably in written form. Consent is obtained only for specific data and for a specific purpose. Granted consent may be withdrawn in accordance with legal regulations.

6. SOME OBLIGATIONS OF THE CONTROLLER, RESPONSIBLE PERSONS, AND OTHER PERSONS WHEN HANDLING PERSONAL DATA 6.1 Every responsible person of the controller is obliged to act in such a way as not to jeopardize the protection of personal data processed by the controller. 6.2 Furthermore, they are obliged to: a) Prevent accidental and unauthorized access to personal data processed by the controller, b) if they discover a personal data breach, unauthorized use or misuse of personal data, or other unauthorized conduct related to personal data protection, immediately prevent further unauthorized handling, in particular, ensure unavailability and report this fact to the statutory representative of the controller and the DPO. 6.3 The statutory representative of the controller is obliged to: a) Prepare and regularly update a security analysis of personal data processing at the controller's, especially from the perspective of collected personal data, authorized persons, and personal data security, b) inform responsible persons about all significant facts, procedures, or events related to personal data handling at the controller's, without undue delay, c) ensure that the controller's responsible persons are properly instructed about their rights and obligations in personal data protection, e) ensure that the controller is able to properly demonstrate the fulfillment of the controller's obligations in personal data protection arising from legal regulations.

7. CONTACTS DPO: Lucie Kalašová, Břidličná 1053/8 Praha 4 Podolí 147 00 ÚOOÚ (Office for Personal Data Protection): Úřad pro ochranu osobních údajů, Pplk. Sochora 27, 170 00 Praha 7