According to provisions of the *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; hereinafter "**GDPR**") Private High School QSI International School of Skopje – Skopje with address Zenevska Str. Number 51, 1000 Skopje, Republic of North Macedonia and registration number 6288065 (hereinafter referred to as: »**QSI**«) hereby adopts the following

PERSONAL DATA PROCESSING AND PROTECTION POLICY

GENERAL PROVISIONS

Article 1

This Policy shall provide organizational, technical, and logical-technical procedures and measures to protect personal data in QSI, with a purpose to avoid accidental or intentional unauthorized destruction of personal data, unauthorized modification or loss of personal data, as well as unauthorized access, processing, use, or transmission of personal data.

QSI provides all the above in the following way:

- the school premises, equipment, and system software, including input and output devices, are secured;
- the application software used for processing personal data is secured;
- access to personal data during physical and digital transmission, is secured;
- procedures for blocking, destroying, deleting, or anonymizing personal data are in place.

All the above are granted by measures taken by QSI according to this Policy.

Employees and external collaborators who process and use personal data during as a function of their employment, must be familiar with the provisions of local laws, the legislation regulating specific areas of their work, and the content of this Policy. Employees must be regularly educated and trained. Employees could be held personally liable for any damage which occurred or criminal acts conducted due to breach of laws and/or this Policy.

Article 2

Terms used in this Policy have the following meaning:

Personal data - means any information relating to an identified or identifiable natural person ('**data subject'**); an identifiable natural person is one who 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;

Filing system - means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

Processing - means any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organizing, structuring, storing, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

The data controller - means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

Special personal data - personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;

Personal data user - means a natural or legal person, public authority, agency, or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with North Macedonian law shall not be regarded as recipients; the processing of data by those public authorities shall follow the applicable data protection rules according to the purposes of the processing.

Data carrier - all types of assets which contain written or recorded data (documents, acts, materials, writings, computer equipment including magnetic, optical, or other computer media, photocopies, audio and visual material, microforms, transmission of data, etc.).

Third party - means a natural or legal person, public authority, agency, or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

Terms not specifically mentioned shall have the same meaning as defined by the GDPR.

SECURING PREMISES

Article 3

Premises where personal data carriers, hardware and software are kept (hereinafter referred to as: "**protected premises**"), must be secured by means of: i) organizational; ii) physical; and iii) technical measures that prevent unauthorized access to data.

Protected premises are protected with:

- alarm system of the entire building (only authorized persons may enter and access the building with a key with one code to switch of the alarm; back gates are closed for public access)
- locking and securing individual premises where personal data or data carriers are located (only authorized persons have the key)
- physical security (security guard and surveillance cameras).

Article 4

Third parties are only allowed to access protected premises in the presence of QSI's employees or other QSI's authorized individual. Carriers and displays of personal data must be placed in a way that a third party does not have access to them and is also not able to gain insight into personal data.

QSI keeps records of persons to which the keys and passwords to the protected premises have been handed over. Each person must confirm the receipt of the keys and password in a written form. Persons who received keys and passwords may not hand over the keys or password to any third party and may not ever leave keys or password in a place where any other persons have access to them. The keys must never be left in the lock of the door from the outside.

Protected premises must not remain uncontrolled, or should, in the absence of workers who supervise them, be locked, and secured according to this Article.

Article 5

Outside working hours and during their absence, QSI's employees or any other authorized person must always lock cabinets and desks where carriers of personal data are kept. Computers and other hardware must be shut down and locked physically and by software.

Carriers of personal data must not be kept in accessible and visible places in the presence of third parties. Carriers of personal data located outside the protected premises (hallways, common areas) should be always locked. Special personal data should not be kept outside the protected areas.

Documentation which contains personal data of employees and is obtained and processed regarding the employment is stored in locked file cabinets in the offices and hallways/locked storage room.

Article 6

Maintainers of premises, hardware and software, visitors, and business partners may only be on the protected premises with the knowledge and in the presence of QSI's authorized person. Cleaners, security guards, etc., may be on those protected premises outside of working hours only where insight into personal data is not possible (data carriers are stored in locked cabinets and desks, computers and other hardware are turned off and physically locked).

Personal data is stored at a local DVR device/server/laptops in secured premises at the address of QSI. Certain data is stored by external provider of QSI: Quality Schools International Ltd., Office 1-2, First Floor, Ardent Business Centre, Triq l-Oratorju, Naxxar, Malta, registered number: C 91823 (QMS Desktop, QMS Web, and other similar platforms).

SECURING SOFTWARE AND HARDWARE

Article 7

Access to the software is protected in a way to permit access only to certain employees (which are predefined) or to legal or natural persons which, based on a contract, provide certain services to QSI.

Article 8

Correction, modification, and updating of system and application software is permitted only with the approval of an authorized person and may be carried out only by authorized services and organizations and individuals which, based on a contract, provide certain services to QSI. Amendments to the system and application software should be properly documented by the provider.

Maintenance and repair of computer hardware and other equipment is only allowed with the knowledge of authorized persons and may be carried out only by the authorized service and maintenance personnel who have concluded an appropriate contract with QSI.

Article 9

The same provisions as for the rest data from this Policy apply also for storage and protection of applicative software.

Article 10

Content of drives of network servers/DVR system and local workstations, where personal data are kept, is regularly checked for the presence of computer viruses or compromised software. Upon the discovery of a computer virus or compromised software, the exploit must be eliminated as soon as possible by professional services of QSI and / or an external contractor, which has concluded an appropriate contract with QSI. The cause of the virus or exploited software in the computer information system must be identified.

All data, personal or otherwise, software, hardware, or other devices, which will be connected or used on any network or information system in QSI, must be quarantined until it can be established that the data, software, hardware, or other device poses no risk to the QSI network or data.

Article 11

Employees may not install software without the knowledge and permission of the person responsible for the operation of a computerized information system. It is not allowed to take the software and/or media on which personal data is kept outside the QSI premises without the approval and the knowledge of the person responsible for the operation of the information system. Whenever taken

outside QSI premises, devices must be protected in the same way as within the QSI premises (kept in a locked cabinets).

To process personal data, as a rule, software and hardware provided by the QSI should be used. In the case where personal data is processed on a private device, the owner of the device must make sure that two accounts are used – one private and one for QSI, to enable QSI to insight business data at any time and without any limitations. Employees need to observe provisions of this policy as well when using their own devices.

It is not allowed to connect to public or unsecure networks if device, whether QSI provided or personal, if used for processing personal data of QSI.

Article 12

Access to the data via application software is protected by usernames and passwords for authorization and identification of program and data users.

Individuals must not use the same password for more than 1 account. Regarding passwords, please follow the following rules: NIST Special Publication 800-63B Digital Identity Guidelines (https://pages.nist.gov/800-63-3/sp800-63b.html).

Data carriers with personal data must have an active full device encryption. Antivirus software must be promptly updated and must be active at any time.

Article 13

For the purpose of restoring a computer system which has been damaged or destroyed, or in the case of other exceptional situations, routine backups (meaning at least once a day) of all data and configurations of local and remote laptops, workstations, servers, devices, and other computer systems shall be undertaken.

Locally stored backups must be stored in specially designated areas, which must be fire-resistant, protected against flooding and electromagnetic radiation, within the prescribed climatic conditions and locked. Additional offsite backups must be similarly stored and protected.

Backups must be maintained for a period of no less than one month.

Article 14

Devices provided by QSI are to be used for business purposes only. Use of devices for private purposes is not recommended. If you choose to use the device for personal use as well, the following must be given special attention and requires consultation with the QSI IT team:

- maintenance of hardware and software
- downloading software
- antivirus protection
- use of professional versions only
- updating of software

EXTERNAL PROVIDERS OF SERVICES

Article 15

Any external natural or legal person who carries out specific tasks related to the collection, processing, storing or forwarding of personal data (data processor) must conclude a written agreement with QSI to ensure the protection of personal data. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

The processor shall not engage another processor without prior specific or general written authorization of the controller. In the case of general written authorization, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data, and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

- processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by North Macedonian law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
- ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- takes all measures required pursuant to Article 32 of the GDPR;
- respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;
- taking into account the nature of the processing, assists the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of GDPR;
- assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of GDPR taking into account the nature of processing and the information available to the processor;
- at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless North Macedonian law requires storage of the personal data;
- makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

RECEIPT AND TRANSMISSION OF PERSONAL DATA

Article 16

An employee who is responsible for receiving and recording of physical mail, must hand over postal items with personal information directly to the individual or department to which it is addressed.

An employee who is responsible for receiving and recording of physical mail, opens and inspects all parcels which in any way arrive at QSI, except shipments in the third and fourth paragraphs of this article.

An employee who is responsible for receiving and recording of physical mail, does not open those shipments that are addressed to another body or organization and are mistakenly delivered, and those shipments which are classified as personal data.

An employee who is responsible for receiving and recording of physical mail shall not open consignments addressed to the employee when the statement on the envelope states that it should be delivered personally to the employee. The same applies for shipments where the first mentioned person on the envelope is personal name of the worker (and then address QSI) without any indication of his official position.

Article 17

Personal data may be transferred electronically and other means only when procedures and measures to prevent unauthorized access or of their contents are implemented.

Sensitive data is transmitted to the addressees in a sealed envelope to the signature on the book or the delivery with acknowledgment of the receipt.

Personal data shall be sent by registered post.

The envelope in which personal data are sent, has to be designed in a way that it is impossible to see the content of the envelope in normal lightning or special lightning (i.e. by backlighting the envelope). The envelope also has to ensure that opening and insight in the content of the envelope cannot be made without leaving trace of opening the envelope.

Article 18

Processing of special personal data must be specially marked and protected.

The information referred to in the preceding paragraph may be provided electronically only if they are specifically protected by cryptographic methods to ensure the illegibility of data during transmission.

Article 19

Personal data shall be provided only to those users who are recognized by the respective legal basis, or by written request or consent of the data subject.

For every transmission of personal data, the recipient must file a written application. The recipient must provide a legal basis (provision of the law) which entitles recipient to obtain such personal data or written request or consent of the data subject.

Original documents may never be transferred, except in the case of a written court order. The original documents must be replaced by a copy during their absence.

RETENTION PERIODS

Article 20

Personal data will be stored and processed:

- for as long as it takes to achieve purposes for which personal data was collected; or
- for as long as it takes for possible claims/disputes to be finally resolved (expiration of statute of limitations or other relevant deadlines); or
- until the permission is withdrawn (only in cases where QSI has no other legal basis for processing personal data); or
- for as long as it is stipulated by the law (in cases when the law defines the retention period).

After the retention period is expired, personal data shall be erased, destroyed, or anonymized, unless the law or another act provides otherwise.

Article 21

The method to delete data from the computer media must provide that it is impractical to restore all or part of deleted data.

Information on traditional media (documents, files, register, lists, etc.) shall be destroyed in a way that makes it impossible to read all or part of the destroyed data.

In the same way supporting materials (e.g., Matrix calculations and graphs, sketches, experimental or unsuccessful extracts, etc.) must be destroyed.

It is prohibited to dispose data carriers with personal data in the general trash.

When transferring data carriers to a place of destruction, adequate insurance during a transfer has to be provided.

Transferring media to a place of destruction and destruction of data carriers shall be controlled by a special committee. The latter must prepare a record on destroying such data carriers.

INTERVENTION WHEN SUSPICION ON UNAUTHORIZED ACCESS OCCURS

Article 22

Employees are obliged to immediately inform an authorized person about activities related to the detection or unauthorized destruction of confidential data, malicious or unauthorized use, appropriation, modification, or damage of such data. Employees are also obliged to prevent any activity from the previous sentence.

QSI is obliged to act according to provisions of the GDPR in case of breach, which stipulates that under certain conditions, QSI has to inform competent authority and subject data.

LIABILITY FOR THE IMPLEMENTATION OF MEASURES AND PROCEDURES

Article 23

Legal representatives of QSI are responsible and liable for implementation of the procedures and measures to protect personal data. Within the scope of their work, department leaders and individual employees are responsible as well.

Article 24

Anyone who processes personal data is obliged to implement the prescribed procedures and measures to safeguard data and protect data, which were provided to him or her during working process. The obligation of data protection does not end with the termination of the employment relationship or other legal basis.

Before taking part in a job where personal data are processed, the employee is required to sign a special declaration, which commits him or her to the protection of personal data.

The declaration from the previous paragraph must provide that the signatory is familiar with the provisions of this policy and the provisions of GDPR. The statement must also include instruction on the consequences of the infringement.

Article 25

Individuals are disciplinary, materially, and criminally liable for breaching provisions of this policy.

FINAL PROVISIONS

Article 26

Draft of this policy has been presented to QSI employees in training in October 2021.

Article 28

This policy shall enter into force 8 days after being presented to employees.

Skopje, *6 October 2021*

Private High School QSI International School of Skopje – Skopje with address Zenevska Str. Number 51, 1000 Skopje, Republic of North Macedonia and registration number 6288065 **(QSI International School of Skopje)**

.....