PROTECTION OF PERSONAL DATA POLICY 2026

Approved by:	Mel Hitchcocks	**Last reviewed on:**	August 2026
Date:	August 2026	**Next review due by:**	August 2027

Our Mission

We provide a **high-quality British style international education** in English, balancing tradition and innovation.

We aim to be the internationally recognized, **outstanding educational choice** for families in the region.

Our passion is creating a **positive, safe and nurturing learning environment** in which everyone is valued as individuals, empowering them to be versatile, motivated and caring people.

We will endeavor to **create opportunities** to develop creativity, collaboration and critical thinking skills through an **inclusive and personalized experience.**

Our Values

Excellence - We strive for excellence in everything we do.

Respect - We learn at school by showing respect to everyone in the community.

Responsibility - We are engaged in promoting actions and behaviours that support a sustainable future.

Integrity - We are transparent, honest and ethical in all our relationships.

Compassion - We are kind and caring, encouraging everyone to succeed.

Rationale

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals in the processing of personal data and on the free flow of such data and on the repeal of Directive 95/46/EC (hereinafter: "General Regulation") and Personal Data Protection Act of the Republic of Slovenia (ZVOP-2) are the laws that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data.

School is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data. This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the legislation. It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

Policy objectives

This policy defines organizational, technical and logistical-technical procedures and measures for securing personal data in the school with the aim of preventing accidental or intentional unauthorized destruction of data, its alteration or loss, as well as unauthorized access, processing, use or transmission of personal data.

The management, employees and all others involved in the work process of the school on the basis of an employment contract or other contractual basis, who process and use personal and/or confidential data during their work and/or become familiar with the business secrets, must respect the provisions of the applicable legislation governing the area of personal data protection and the provisions of the legislation governing the individual areas of their work and the content of this policy. Before starting to work in the school, the employee must sign a declaration obliging him to protect personal data. It must be clear from the signed statement that the signatory is familiar with the provisions of this policy, the General Regulation, and the Slovene legislation. The statement must also contain instructions on the consequences of violating the provisions.

The declaration shall also be signed by:

- the school's external employees who, while performing contractual work, become familiar with, or could become familiar with, personal data managed by the school.
- all students working (interns), volunteers and external interns who become familiar with personal data in the context of cooperation with the school.

The policy is published on the School's SharePoint and sent to all employees via e-mail.

Definitions

Terms used in this policy have the following meanings:

- ***Personal data*** means any information relating to a specific or identifiable individual (hereinafter: " data subject");
- *An **identifiable individual*** is an individual who can be identified directly or indirectly, in particular by reference to an identifier such as name, 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 this individual;

- *A **breach of personal data protection*** means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data that is sent, stored or otherwise processed;
- ***Data carrier*** means all types of means on which data is recorded or recorded (documents, files, computer equipment including magnetic, optical or other computer media, photocopies, audio and visual material, microfilms, data transfer devices, etc. .);
- ***Processing*** means any operation or set of operations which is performed on personal data or 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;
- ***Processor*** means a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller;
- ***Data concerning health*** means personal data relating to the physical or mental health of an individual, including the provision of health services, which reveal information about the individual's health status;
- ***Special types of personal data*** are personal data revealing racial or ethnic origin, political opinion, religious or philosophical belief or trade union membership, and the processing of genetic data, biometric data for the purpose of unique identification of an individual, health-related data or data related to with the individual's sex life or sexual orientation;
- ***Consent*** means any freely given, specific, informed and unambiguous declaration of will of the individual to whom the personal data relates, by which he/she expresses consent to the processing of personal data relating to him/her by a statement or a clear affirmative action;
- ***Third person*** means a natural or legal person, public authority, agency or body other than the data subject, the controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data;
- ***User*** means a natural or legal person, public authority, agency or other body to whom personal data has been disclosed, regardless of whether it is a third party or not. However, public authorities that may receive personal data in the framework of a particular inquiry in accordance with Union or Member state law shall not be considered as users; the processing of those data by those public authorities takes shall be in compliance with the applicable data protection rules according to the purposes of the processing;
- ***Controller*** means a natural or legal person, public body, agency or other body which, alone or jointly with others, determines the purposes and means of processing of personal data; when 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 member state law.

PERSONAL DATA PROCESSING

Personal data is any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the information. The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of a living individual. Personal information also includes an identifier such as a name, an identification number, location data or an online identifier.

The school collects and processes personal data of Employees, Students, Parents and Business Partners. Personal data include student records, staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection,....

Some of the personal data the school process is classified as specific categories of personal data (sensitive data). This means personal data about an individual's, health data, special education support data, religion and ethnic origin.

Lawful Basis for processing personal information

Personal data may be processed in the school if at least one of the following conditions is met:

- **Consent:** the individual to whom the personal data relates has given consent to the processing of his personal data for one or more specified purposes;
- **Contract:** the processing is necessary for the performance of a contract to which the individual is a contracting party, or in order to take steps at the request of such an individual prior to entering into contract;
- **Legal obligation:** processing is necessary to fulfill a legal obligation applicable to the controller;
- **Vital interest:** processing is necessary for protection vital interests of the individual to whom personal data refer or of another person;
- **Public task:** processing is necessary for the performance of a task in the public interest or in the exercise of official authority vested in the controller;
- **Legitimate interest:** processing is necessary due to the legitimate interests pursued by the controller or by a third party, except when such interests are overridden by the interests or fundamental rights and freedoms of the individual to whom the personal data relate, which require protection of personal data, in particular when the individual is a child.

Personal data may only be processed for specified and lawful purposes and may not be further processed in such a way that their processing is inconsistent with these purposes unless the law provides differently.

When processing special types of personal data, employees must be especially conscientious and careful. Special types of personal data must be protected in such a way that unauthorized persons are prevented from accessing them.

The individual must be informed about the processing of personal data and his rights must be presented to him, both in accordance with the General Regulation.

Rights for 'data subjects'

Individuals have the following personal data protection rights:

- **The right to be informed:** They may request information about whether the organization has personal data about them and, if so, what data it has and on what basis it has it and why it uses it.
- **The right to access:** They can request access to their personal data, which allows them to receive a copy of the personal data that organizations hold about them and to check that the organization is processing it lawfully.
- **The right to rectification:** They may request corrections of personal data, such as corrections of incomplete or inaccurate personal data.
- **The right to erasure ("right to be forgotten")**: They can request deletion of personal data when there is no reason for further processing or when they exercise their right to object to further processing.
- **The right to object:** They can object to the further processing of personal data where the data is processed on the basis of a legitimate interest (even in the case of a third party's legitimate interest), when there are reasons related to their special situation. Regardless of the provision of the previous sentence, they have the right to object at any time if the organization processes their personal data for direct marketing purposes.
- **The right to restriction of processing**: They can request the restriction of the processing of personal data, which means stopping the processing of personal data about them, for example, if they want the organization to determine its accuracy or check the reasons for its further processing.
- **The right to data portability:** They may request the transfer of personal data in a structured electronic form to another controller, if this is possible and feasible.
- They can **revoke the consent** they gave to the collection, processing and transfer of personal data for a specific purpose; upon receiving notification that they have withdrawn their consent, the organization will stop processing their personal data for the purposes they originally consented to, unless the organization has no other lawful legal basis for continuing to lawfully process the data.

The school is obliged to ensure that individuals are informed about the rights above in an appropriate manner that is consistent with the requirements of the General Regulation. The school is obligated to communicate any rectification or erasure of personal data or restriction of processing to individual to whom the personal data have been disclosed unless this proves impossible or involves disproportionate effort.

The school also provides a single point of contact that individuals can turn to and communicate when exercising their rights. If an individual wishes to exercise any of the rights, he can send a request by e-mail to the address: enquiries@britishschool.si or by regular mail to the address of the school.

The school informs the individual who is exercising his rights with the request, of the decision and of the personal data, if this is the subject of the request. The information will be provided in writing or by other means, including, where appropriate, by electronic means. School will provide information without undue delay and in any event within one month after receiving the request. If necessary, this

deadline can be extended by a maximum of two additional months, considering the complexity and number of requests. The school informs the individual about the extension of the deadline. The School's decision must contain reasons and information about the right to appeal to the Information Commissioner within 15 days of being informed of the decision.

Access to one's own personal data and exercising rights is free of charge. Where the data subject's requests are manifestly unfounded or excessive, particularly because they are repeated, the school may charge a reasonable fee, considering the administrative costs of providing the information or message or taking the requested action, or refuse to act on the request.

In the case of exercising rights, the school may need to request certain information from the individual to confirm the individual's identity, which is only a security measure to ensure that personal information is not disclosed to unauthorized persons.

If an individual believes that his rights have been violated, he can turn to the supervisory authority for protection or assistance. He can turn to the Information Commissioner: gp.ip@ip-rs.si or find information on the website: www.ip-rs.si.

Transfer of personal data

School transfers personal data to the public sector entities or other natural or legal entities, if there is an appropriate legal basis for the transmission in accordance with the law, unless another law provides otherwise. The recipient of the data may only process the personal data for the purpose for which they are forwarded to him.

The transfer of personal data must be requested by the applicant in writing. The request must contain:

- information about the applicant (for a natural person: personal name, address of permanent or temporary residence; for a self-employed individual, an individual carrying out an activity independently, and for a legal entity: title or company and address or registered office and registration number) and the signature of the applicant or authorized persons;
- the legal basis for obtaining the requested personal data;
- the purpose of processing personal data, or the reasons that demonstrate the necessity and suitability of personal data to achieve the purpose of acquisition;
- identification of the matter in connection with which personal data is required, and indication of the authority or other entity handling the matter;
- the types of personal data to be provided to him;
- the form and method of obtaining the required personal data.

Unless otherwise stipulated by another law, the school shall provide the applicant with the requested personal data no later than 15 days after receiving a complete request, or shall inform

the applicant in writing within this period of the reasons for not providing the requested personal data. The school and the applicant can agree on its extension within the deadline. If the school does not provide data within 15 days or if the deadline is not extended, the request is considered rejected.

Personal data provided to the user in physical form must be provided in an envelope. Special envelopes must be used, so that the opening of the envelope and familiarization with its contents cannot be done without a visible trace of the opening of the envelope.

Personal data may only be transmitted by information, telecommunication and other means when procedures and measures are implemented to prevent unauthorized persons from misappropriating or destroying data and from unauthorized access to their content.

Special types of personal data are sent in physical form to addresses in sealed envelopes by registered mail with a return receipt request. If special types of personal data are sent in electronic form, their unreadability must be ensured during transmission, so that they are encrypted and protected with a password.

An employee who processes personal data is obliged to record every transmission of personal data outside the school. In the record of data transmission, which personal data was transmitted, to whom, when and on what legal basis and for what purpose or the needs of which process.

PROTECTION OF PERSONAL INFORMATION

The protection of personal data shall cover the legal, organisational and appropriate logistical and technical procedures and measures to:

- Protect premises, hardware and system software,
- Protect the application software used to process personal data,
- Ensure the security of the transmission and transfer of personal data,
- Prevent unauthorized persons from gaining access to the devices on which personal data are processed and to the personal data files,
- Permit the subsequent identification of when individual data were used and entered in the database and by whom, for the period for which the individual data are stored.

When it is possible that the planned processing of personal data, especially with the use of new technologies, considering the nature, scope, circumstances and purposes of the processing of personal data, could cause a high risk to the rights and freedoms of individuals, the IT Manager shall be alerted to this. In this case, an implementation assessment in relation to data protection, as defined in Article 35 of the General Regulation and the applicable legislation in the field of personal data protection, is carried out.

Mail security

The employee who oversees receiving and recording mail in the school must hand over the mail with personal data directly to the individual or department to which the mail is addressed. He/she also opens and inspects all postal shipments and shipments addressed to the school that arrive at the school in another way (e.g. brought by customers or couriers), except for shipments from the second and third paragraphs.

The employee who oversees receiving and recording mail does not open those shipments that are addressed to another authority or organization and are delivered by mistake, as well as those

shipments that are marked as personal data or for which it follows from the markings on the envelope that they refer to tender.

The employee who oversees receiving and recording mail may open shipments addressed to the address of the school and the employee at the same time, except in cases where it is clear from the envelope that the mail must be delivered to the employee personally.

Events

For the purposes of recording activities and informing the public about work and events in the school, such as events, meetings, competitions, trainings and the like, school may partially or fully record or photograph such an event and publish the produced material on the school's websites, newspapers and social networks.

The notification that the event will be filmed or photographed is written on the invitation or on the notification of the event. The purpose of recording or photographing is also stated. In this way, it is considered that the participants or visitors are informed about the filming or photography of the public event.

When this is more appropriate (at events with a smaller number of participants, events that are not open to the public, and the participants reasonably expect a higher level of privacy), recording or photography is announced verbally, and participants are given the opportunity to express their will regarding the capture of their image with the camera.

Training

School regularly informs employees about the importance and innovations in the field of personal data protection and conducts training in this field and in the field of information security. School presents the following to employees once a year:

- the rights and duties of employees regarding the protection of personal data,
- dangers and the most common risks for the protection of personal data,
- possible consequences for the school and employees in the event of a data protection breach,
- password protection and password management,
- protection of equipment and premises,
- safe handling of data outside the school's premises (e.g. on laptops, smartphones, USB keys, etc.),
- clean table policy,
- other practices, policies and cases in the field of personal data protection.

The school regularly implements security policies in the field of information security, which are defined in internal acts and checks them at least once a year.

Contractual processing of personal data

A written contract or other legal act is concluded with each external legal or natural person that performs individual tasks related to the processing of personal data for the school in accordance with law. Contract determines the obligations of the processor towards the controller. The contract specifies the content and duration of processing, nature and purpose of processing, type of personal data, categories of individuals to whom personal data refer, and

obligations and rights of the controller. The content of such a contract is more precisely determined by Article 28 of the General Regulation.

Processors are also external collaborators who maintain hardware and software and manufacture and install new hardware or software in case they have access to personal data in the course of their work.

External legal or natural persons may perform personal data processing services only within the scope of the school's authorization and may not process or otherwise use personal data for any other purpose.

An authorized legal or natural person who provides agreed services for the school outside the operator's premises must have at least as strict a method of ensuring the security of personal data as specified in these regulations.

Data deletion

Personal data may only be processed for as long as the retention period is specified, or as long as there is a legal basis. School limits the retention period of personal data to the shortest possible period and only as long as the retention is necessary to achieve the processing purpose for which the data was collected or further processed. After the storage period has expired, personal data is deleted, destroyed, blocked or anonymized or another procedure is carried out that makes it impossible to identify the individual, unless the law or another act stipulates otherwise.

Personal data processed by the school **on the basis of a contractual relationship** with an individual is kept by the school for the period necessary for the execution of the contract and for 6 years after its termination, except in cases where a dispute arises between the individual and the school regarding the contract. In such a case, the school keeps the data for 10 years after the finality of the court decision, arbitration or settlement or, if there was no legal dispute, for 6 years from the date of the peaceful resolution of the dispute.

Personal data that the school processes **on the basis of the individual's personal consent** or legitimate interest will be kept until this consent is revoked or until the deletion is requested. In the event of cancellation or a justified request for deletion, the data will be deleted without undue delay after the school has decided on the individual's request. School may delete this data even before cancellation, when the purpose of personal data processing has been achieved or if the law so requires.

In the event that the School receives a request from an individual regarding his rights from the General Regulation, the school may not delete, dispose of or change the requested personal data that is the subject of the procedure, processing logs and other related information, regardless of the course prescribed or internally determined retention periods, until the case has been finally decided, and after the final decision, acts in accordance with the final decision in the case.

Exceptionally, school may refuse a request for deletion for reasons from the General Regulation, as listed below:

- exercising the right to freedom of expression and information,

- fulfillment of the legal obligation of processing,
- reasons of public interest in the field of public health,
- archiving purposes in the public interest,
- scientific or historical research purposes or statistical purposes,
- exercising or defending legal claims.

To delete data from data carriers, such a deletion method is used that it is impossible to restore all or part of the deleted data.

Data on classic media (documents, files, register, list, etc.) is destroyed in a way that makes it impossible to read all or part of the destroyed data. Auxiliary material (e.g. matrices, calculations and charts, sketches, trial or unsuccessful printouts, etc.) is destroyed in the same way. It is forbidden to

dispose of waste data carriers with personal data in the trash. When transferring personal data carriers to the place of destruction, it is necessary to provide adequate insurance even during the transfer. The transfer of data carriers to the place of destruction and the destruction of personal data carriers is supervised by a special commission, which also draws up an appropriate report on the destruction, or the destruction is handed over to the appropriate external service based on the concluded contract.

Information security policy

Employees use various information technology (computer, phone, tablet and other electronic devices) and various electronic services (internet access, e-mail, cloud access, shared directories and folders and other software or services) assigned to them exclusively by the employer for business purposes.

To a limited extent and within reasonable limits, information technology and electronic services provided by the school may also be used for private purposes. In doing so, employees must protect the school's reputation, and technologies and services must not be used for inappropriate or offensive purposes. The Principal may, at their own discretion, prohibit an employee from using it for private purposes at any time.

World Wide Web

Access to the World Wide Web is provided to employees for their work, education and information.

Employees must use the World Wide Web in accordance with ethical and moral norms. All users of information systems must be aware that they identify themselves on the Internet with the network address of the public institution body (IP address).

Forwarding work e-mail addresses to external web servers for the purpose of registering for a specific service (e.g. mail, registering for training, etc.) is not permitted, unless it is related to the school's business process.

In the school's network, at the request of the responsible person, statistics of visited websites can be produced, which must be anonymized and not for public publication. The statistics may be used exclusively for the planning and protection of the information system.

To ensure information security and the availability of information resources and to prevent violations, the school can order the blocking of certain websites. Access to certain websites is blocked by the IT Manager, based on a written order from the Principal. All employees are notified of the blocking by e-mail.

Work e-mail

The official e-mail can be used in the school as a tool for communication with parents, students, employees and external contractors. In doing so, workers must adhere not only to ethical and moral norms, but also to etiquette. The sender must be aware that any message from the recipient's work e-mail address may be considered the opinion of the organization in which the sender is employed.

Employees may not send chain letters and large files (music, movies, plays, startup files and scripts, etc.) by e-mail, if they are not intended for work.

Employees may not use their work e-mail address for marketing purposes and may not use it to send advertising mail to known and/or unknown addresses. Also, employees may not sign up for promotional mail or newsletters using the school's email addresses, unless it is related to the needs of the workplace.

Employees should be careful when opening e-mails with attachments from unknown senders. If it is suspected that it is spam, which could be harmful, it should not be opened, but the IT Manager should be notified immediately.

Employees must not send special types of personal data or passwords by e-mail, except in properly accredited systems, or their unreadability must be ensured during data transfer, so that they are encrypted and protected with a password.

Private e-mail

The use of private e-mail (e.g. Gmail, Yahoo , etc.) for work purposes is prohibited, as it potentially constitutes unauthorized processing of personal data. Exceptionally, it is permitted to use private e-mail exclusively for the purposes of communication between employees and the Human Resources department.

Work mobile phones and telephones

Mobile phones that are owned by the school and used by employees should not be tracked. No tracking devices or applications may be installed on mobile devices.

Access to the work telephone usage data from operators of telecommunications services is allowed only when there is any dispute between school and the employee regarding the amount of the costs of using a specific telephone connection.

Access to computer by third person

The IT Manager may, upon a specially justified written request of the Principal in the presence of a three-member committee, in extraordinary cases (sudden resignation of an employee, death of an employee, unexpected, sudden and prolonged or permanent absence of an employee, termination of employment by employee without a notice period, termination of the employment due to reasons of fault due to unexcused absence and in similar extraordinary cases) access to information technology (e.g. computer) or other electronic services (e.g. e-mail) of the employee only if this is absolutely necessary to fulfill the legal obligations of the school or to manage the work process.

The inspection is carried out by a three-member commission, appointed each time by the Principal. It must include at least one employee representative who is not a part of the Senior Leadership Team (SLT). The commission must write a report on the inspection, which contains:

- explanation of the reason for the inspection,
- record of entry with any comments of the worker, if present,
- statements of persons present,
- a list or a printout of the obtained data.

If there is reasonable suspicion that employees do not comply with the provisions of the information security policy of this policy, the IT Manager may, upon a specially substantiated written request of the Principal, control the use of electronic services, but only from the point of view of reviewing the diary records of the amount traffic and stored data that load the server. In doing so, the contents may not be reviewed.

The employee must be informed in writing about the purpose of using information technology and electronic services and the possibility of inspection. A notice together with these rules sent to all employees by e- mail is considered sufficient notice.

Return of work information technology

Upon termination of the employment the employee is obliged to return the work information technology that he used for official purposes. Before returning the equipment, the employee must ensure that all private content is cleaned or deleted, but official content preserved.

Use of personal information technology devices

In addition to work equipment, the employee may use his personal equipment and other technical devices (mainly mobile phone) for the purposes of performing work, if such use is approved by the Principal and the employee gives voluntary written consent that the employer may process his private telephone number or private email address for the purposes of performing the work process.

In the event of termination of the employment relationship, the employee is obliged to delete all work-related personal data on his personal equipment or other technical devices (mainly mobile phone) that he used for the purposes of performing work in agreement with the employer.

Security of premises

Network room

The network room in which hardware and software is located must be protected by organizational and physical and/or technical measures that prevent unauthorized persons from accessing the data.

Access to the network room is possible only during regular working hours, and outside of these hours only with the permission of the Principal and the IT Manager. The room must not remain unattended, it must be locked in the absence of the workers supervising them.

The keys to the secure premises are used and kept in accordance with the house rules. The keys are not left in the lock in the door from the outside.

Principal and Administration area

Rooms that are intended for meetings with visitors (Parents, Staff and others) are **Principal room, Admin area and Reception room in new building** (hereinafter: secure premises). Secured premises in which personal data carriers, hardware and software are located must be protected by organizational and physical and/or technical measures that prevent unauthorized persons from accessing the data.

Access to these premises is possible only during regular working hours and outside of working hours only with the permission of the Principal. They must not remain unattended; they must be locked in the absence of the workers working there. Non-employees (including maintenance staff, business partners, parents) may not enter secure areas without being accompanied by a

member of staff. The keys to the area are used and kept in accordance with the house rules. The keys are not left in the lock in the door from the outside.

Employees must not leave their workplace unattended or unlocked, or they must ensure that original documents and personal data carriers are stored in such a way that unauthorized persons do not have access to them. Outside of working hours, cabinets and desks with personal data carriers must be locked (clean desk policy).

Computers and other information technology or equipment that allows access to personal data must be either turned off or physically or software locked during the employee's absence (clean screen policy). Data carriers and computer screens must be installed in such a way that visitors do not have a direct view of them.

Employees must not leave personal data carriers on their desks in the presence of people who do not have the right to view them. Personal data of an individual, for which the school does not have a legal basis for their publication, must not be written on boards or in any other way, so that unauthorized persons could become familiar with them.

Classrooms

Computers and other information technology or equipment that allows access to personal data must be either turned off physically or software locked during the employee's absence (clean screen policy). After school hours employees must store computers in cabinets and not leave them on their desks.

Personal data of an individual, for which the school does not have a legal basis for their publication, must not be written on boards or in any other way, so that unauthorized persons could become familiar with them.

Other areas

Holders of personal data located outside of protected areas (e.g. lobby, corridors, common areas, classrooms, lecture halls, dining rooms) must be permanently locked in cabinets. Special types of personal data must not be stored outside of secure areas.

Maintenance and repair

Maintenance and repair of information technology, electronic services and other equipment is permitted only with the knowledge of the IT Manager. It can be carried out by authorized repairer or maintenance personnel who have an appropriate contract with the School or the Orbital Education group.

Maintainers of premises, information technology or hardware and software, visitors and business partners may move to secured premises only with the knowledge of the responsible person.

Workers, such as cleaners, security guards, etc., can only move outside of working hours if access to personal data is prevented (data carriers are stored in locked cabinets and desks, computers and other hardware are switched off or otherwise physically or software locked).

Security of system and application software computer equipment

Access to system and application software must be protected in such a way that it allows access only to IT Manager of the School or to external organization who will perform the agreed services in accordance with the contract.

Repairs, modifications and additions to the system and application software is permitted only on the basis of the approval of School Board. It can only be carried out by an authorized service provider who has an appropriate contract with the School or Orbital group. Contractors must properly document the implemented changes and additions to the system and application software. If it is necessary to make copies for the work, they must be properly destroyed after the end of the purpose for which they were made. The same applies to other printouts, data exports or other tools for performing the servicing service.

The contents of data carriers on network servers and local workstations where personal data is located should be regularly checked for the potential presence of computer viruses and other forms of malicious code. If a computer virus is detected, every effort should be made to eliminate the virus with

the help of specialists and to determine the cause of the virus. All personal data and software that is intended for use in a computer information system and arrive at school on computer data transmission media or via telecommunications channels must be checked for the presence of computer viruses before use.

Employees may not install software without the approval of the IT Manager. They may also not take the software out of the school without the approval of the Principal and the knowledge of their Manager.

Password system

Access to data and use of system and application software is protected by a password system for authorization and identification of software and data users. Each user has his own password for accessing individual electronic services. Lending passwords and using group passwords is prohibited.

The following rules must be observed when generating or setting passwords:

- passwords must have a minimum of 6 characters or more, insofar as this is specified for each user solution;
- passwords must not contain meaningful alphanumeric sequences of characters (e.g. 123456, abcdefg ...);
- Password must not contain the user's account name or more than two consecutive characters from the user's full name.
- passwords must be of good quality (adequate length, upper and lower case letters, numbers, and special characters);
- Password should contain characters from three of the following four categories: Uppercase characters A-Z (Latin alphabet), Lowercase characters a-z (Latin alphabet), Digits 0-9, o Special characters (!, $, #, %, etc).
- passwords should be changed regularly;
- passwords should not be cyclical and should not be repeated from previous periods;
- initial passwords are changed upon first login;
- passwords generated by an external supplier must be changed immediately upon first use in a production environment;
- the user name must not indicate any special authority of the user.

When handling passwords, it is mandatory to follow the instructions:

- the authorized person assigning passwords must treat them confidentially, must prevent the possibility unauthorized access and forward them in a secure manner;
- users must be able to change their user password at any time;
- the password must never be displayed on the screen;
- passwords must be stored in encrypted form;
- passwords must not be stuck to the monitor or stored under the keyboard;

- each user must have their own username and password exclusively for personal use;
- the password must be stored in a way that completely disables another person possibility of insight;
- each user is responsible for the confidentiality of the password and may not entrust it to another person under any circumstances;

- under no circumstances may the user give out the password to a superior, subordinate or person replacing him or to IT staff;
- in case of disclosure of the password or suspicion of disclosure of the password, he must report this immediately authorized person for assigning passwords.

All passwords and procedures used to enter and administer the network of personal computers (supervisor or control passwords), administer e- mail and administer application programs are kept in a safe in a closed envelope or in another appropriate way, so that access by unauthorized persons is prevented. They should only be used in exceptional circumstances or emergencies. Any use of these passwords may be authorized by the Principal. After each such use, a new password content is determined.

ACTION IN CASE OF SUSPECTED PERSONAL DATA PROTECTION VIOLATION

To demonstrate compliance with the General Data Protection Regulation (GDPR), we need to have an effective system in place to detect and communicate personal data breaches. We are obliged to inform the Information Commissioner of the Republic of Slovenia about detected breaches of personal data protection, if it is (at least) likely that the rights and freedoms of individuals would be endangered by the breach. **Notice must be made immediately after a breach is detected, but no later than within 72 hours.**

What is a personal data breach?

Personal data breach means a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to personal data that is transmitted, stored or otherwise processed. The violation may be committed unintentionally (e.g. due to negligence) or it may be planned or intentional. In general, a breach **represents a security incident** that compromises the confidentiality, integrity, and availability of personal data.

Cases that are treated as a security incident as cited by the Information Commissioner are, for example:

- access to personal data by an unauthorized person;
- forwarding personal data to the wrong addressee;
- loss or theft of computer equipment (laptop, USB flash drive, etc.) containing personal data;
- unauthorized destruction of databases with personal data;
- changing personal data without the necessary permission;

- loss of access to personal data (loss of password; loss of decryption equipment; unauthorized installation of an encryption program that disables access to data, the so-called "ransomware virus"), etc.

Employees are obliged to monitor and pay attention to possible security incidents in their work and to act accordingly in accordance with these rules and instructions. When employees notice that a security incident has occurred in school, they must immediately inform the Principal.

Informing the management of the organization

Employees are obliged to **immediately inform Principal Melanie Hitchcocks (mail: mel.hitchcocks@britishschool.si, phone 040 666 723)** about activities related to the discovery,

unauthorized access or destruction of data, malicious or unauthorized use, appropriation, modification or damage, and they themselves try to prevent such activity.

In the event of a security incident, the contact person will document the breach of personal data protection, record further urgent measures or notifications, and carry out further steps, including reporting the breach to the Information Commissioner of the Republic of Slovenia. In the event of a detected breach, it will immediately consult with a GDPR consulting provider to prepare an assessment of the likelihood and severity of the consequences for the rights and freedoms of individuals. The school GDPR consulting provider is company Datainfo d.o.o.

All employees are obliged to assist the contact person in gathering information about the event and to try to limit or eliminate harmful consequences as soon as possible.

Notice to the Information Commissioner

If the school assesses that the incident will pose a risk to the rights and freedoms of individuals, it must **notify the Information Commissioner without delay, but no later than 72 hours after the detected violation.** If the incident occurred in relation to data in which the school acts as a contractual processor, we must notify the data controller (client) of the violation as soon as possible after detecting the violation.

When it is not possible to provide all the necessary information about the incident within the scheduled time of 72 hours, as required by the General Regulation (GDPR), the controller may submit a notification of breaches to the Information Commissioner in stages, but without delay. We are expected to carry out our obligations regarding the investigation of security incidents as a matter of priority and expeditiously. In the event of a delay of 72 hours, we must provide a specific explanation for the delay.

The notification to the Information Commissioner shall contain at least the following information, as required by the General Regulation (GDPR):

- description of the type of incident, category and approximate number of individuals to whom

  personal data relate, the types and approximate number of personal data records;
- contact details,
- a description of the likely consequences of a personal data breach;
- a description of the measures taken by the controller or of the measures envisaged to mitigate the

  risks of violations.

The notification may also contain other important information.

Notice to individuals

Where a personal data breach is likely to result in **a high risk to the rights and freedoms of individuals**, the General Data Protection Regulation (GDPR) requires us to notify the individuals concerned of the breach directly and without delay.

Before deciding on informing individuals, we will consider the opinions and guidelines of the Information Commissioner of the Republic of Slovenia.

The **notice itself to individuals** must contain at least, in clear and plain language:

- the contact details of the authorised person (or other contact person) from whom the individual can receive more information or explanations about the breach,
- information on the consequences,

- information on the measures taken or proposed and, where possible, additional explanations to individuals on how they can reduce the risk of consequences themselves.

Log of security incidents

We will keep a special record of security incidents and accompanying documentation, including such incidents that have not been reported to the supervisory authority or individuals.

The list of notifications on security incidents should contain at least the following information:

- the date of the violation,
- the date on which the incident became known;
- the date of notification to the Information Commissioner (if notification was necessary),
- Internal document/notification number (if any)
- a brief description of the incident;
- a description of the measures.

Failure to act on a detected violation

Failure to act in the event of a detected breach of personal data protection and unjustified failure to notify the Information Commissioner of the Republic of Slovenia of the supervisory authority, when necessary, constitutes an independent violation under the General Regulation (GDPR) and the Personal Data Protection Act ZVOP-2, for which a fine is prescribed.

RESPONSIBILITY FOR THE IMPLEMENTATION OF SECURITY MEASURES AND PROCEDURES

The school takes compliance with this policy very seriously. All employees, as well as external contractors who have signed a cooperation agreement with the company, are responsible for the implementation of procedures and measures to secure personal data. Supervision over the implementation of the procedures and measures specified in these regulations is carried out by Principal or a person authorized by the Principal.

Every employee who processes personal data is obliged to implement the prescribed procedures and measures for securing data and to protect data that he/she has learned about or was aware of while performing his or her work. The obligation to protect data does not end with the termination of the employment or other contractual relationship.

In the event of violations of the provisions of this policy, the employee is liable to compensate the school for damage caused or to persons with whom the school cooperates.

Any failure to comply with any part of this policy may lead to disciplinary action under the school's procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect. Violation of the provisions of the regulations may also result in criminal, misdemeanor and/or compensatory liability of the employee or the person who violates these regulations.

REVIEW AND EVALUATION

This policy is to be reviewed and evaluated annually by SLT, Principal and with the Director of Education, and updated as and when changes occur.

Due for Review: 04/02/2027

PREPARED BY: Mel Hitchcocks, Principal **04/02/2026**