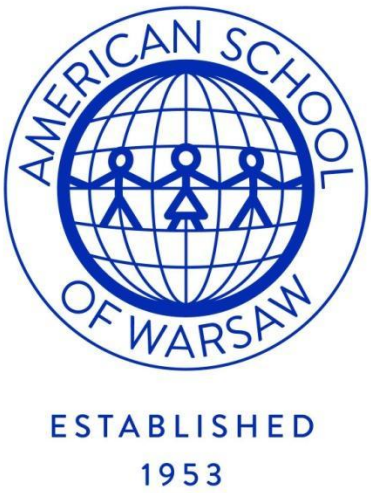

ASW Data Protection Policy & Procedures

Current Version Date	**Next Projected Revision Date**	**Issuing date / Effective date**
February 2021	September 2021	February 2021
Prepared by	**Checked by**	**Approved by**
Data Protection Committee	DPO, Data Protection Committee, Legal Review, School Director	Jon P. Zurfluh Director

ASW Mission Statement

We're determined to be a community that changes the world for the better.

Here, it's all about what you can do rather than what you can't; where every student, at any level of ability, from any culture, is happy and excited because they can choose how they want to learn, not just what they want to learn.

It's a school where asking the right questions is more important than memorizing the right answers; where you make friendships that last a lifetime; and develop life skills that send you out into the world with enough self-belief to change it for the better.

Rationale

As indicated in board policy, the American School of Warsaw (ASW) is committed to the protection of all personal and sensitive data for which it holds the responsibility of as the Data Controller.

This policy is in place to provide the school with the organizational procedures for managing such data in compliance with data protection principles stipulated by the EU General Data Protection Regulation (GDPR) 2016/679 as well as in the Polish Act on Personal Data Protection of 10 May 2018.

Table of contents

Objective and Legal Framework

The policy aims to provide the general framework for ensuring an adequate level of protection for personal data of students, parents or legal guardians of students, employees, and contractual partners processed by ASW.

In addition, the policy provides guidelines to ensure that ASW:

- Complies with data protection law, including GDPR and the Polish Act on Personal Data Protection and follows good practice.
- Protects the rights of employees, students and parents, and other contractual partners.
- Is transparent about how it stores and processes individuals' personal data.
- Implements adequate safeguards to protect itself and individuals whose personal data is processed.

It is mandatory for all staff who have access to any type of personal data to ensure that all their actions comply with the guidelines set out by this policy. The policy will be communicated to all employees and will be public for the entire community.

The policy applies to the data collected from:

1) All ASW employees
2) All contractors, suppliers and other people working on behalf of ASW
3) All students/parents
4) Visitors.

The policy shall apply only where it provides supplemental protection for personal data processed by ASW. Where applicable local law provides more protection than this policy, local law shall prevail.

Policy Framework

The work of this operational policy is linked and an extension of the following board policy:

5.03 Personal Data Protection

The School is committed to the protection of all personal and sensitive data for which it holds responsibility of as the Data Controller. The School will maintain organizational procedures for handling such data in compliance with current data protection principles and the European General Data Protection Regulation (GDPR) 2016/679.

The School will be transparent about the intended processing of data and communicate these intentions by notifying staff, parents, and students prior to the processing of an individual's data. The School will recognize all individuals' legal rights to request access to their data or the information being held and will respond in a timely manner.

The requirements of this policy are mandatory for all staff employed by the School and any third party contracted to provide services to the School. The School Director will ensure that staff are aware of operational data protection policies and procedures.

Changes to data protection legislation shall be monitored and necessary updates implemented to remain compliant with all relevant requirements.

Revised: June 2018

Terminology

- **personal data**: any information relating to an identified or identifiable natural person; 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.

- **sensitive personal data:** any information relating to an identified or identifiable natural person revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data. Data relating to criminal offenses and convictions are addressed separately (as criminal law lies outside the EU's legislative competence).

- **data processing:** any operation or set of operations which is performed on personal data or on 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.

- **restriction of processing:** the marking of stored personal data with the aim of limiting their processing in the future.

- **data controller:** 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.

- **data processor:** a natural or legal person, public authority, agency or another body which processes personal data on behalf of the controller.

- **data recipient:** 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 Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

- **data subject:** A natural person whose personal data is processed by a data controller or data processor.

- **third party:** 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.

- **consent:** any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- **data breach:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed
- **representative**: a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27 GDPR, represents the controller or processor with regard to their respective obligations under this Regulation.
- **DPO**: Data Protection Officer
- **GDPR:** Regulation (EU) 2016/679 of the European Parliament and of the Council, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and follows good practice. Any additional terms related to data protection shall have the meaning designated to them under article 4 of the GDPR.
- **data map:** relevant information of all data processing services, and software associated with the storage and processing of personal data.

Personal data processing principles

In accordance with the requirements outlined in the GDPR, personal data will be:

- **Processed lawfully, fairly and in a transparent manner** in relation to individuals. Thus, the legal basis for processing data will be identified and documented prior to data being processed. Under the GDPR, data will be lawfully processed under one of the following conditions:
    - The consent of the data subject has been obtained.
    - Processing is necessary for:
        - Compliance with a legal obligation.
        - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
        - For the performance of a contract with the data subject or to take steps to enter into a contract.
        - Protecting the vital interests of a data subject or another person.
        - For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.
- **Collected for specified, explicit and legitimate purposes** and not processed further than for the purpose for which it was collected; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

ASW will process personal data only if one of the following circumstances is met:

- The individual whom the personal data is about has consented to the processing.
- The processing is necessary in relation to a contract which the individual has entered into.
- The processing is necessary because of a legal obligation.
- The processing is necessary to protect the individual's "vital interests".
- The processing is necessary for administering justice or for exercising statutory/governmental or other public functions.
- The processing is in accordance with the legitimate interests of ASW or a Third party. However, if doing so would materially prejudice the rights, freedoms or legitimate interests of the persons to whom the data relate, ASW will not process any personal data purely for the purposes of their own legitimate interests.

- **Adequate, relevant and limited** to what is necessary in relation to the purposes for which they are processed.
- **Accurate and, where necessary, kept up-to-date**: every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. ASW will promote an easy procedure for data subjects to update their information.
- **Limited storage.** Personal data will be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Unrequired data will be deleted as soon as practicable.

  Personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of the appropriate technical and organizational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- **Processed in a manner that ensures appropriate security** of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures. This includes both technical and organizational measures such as defined processes and training and awareness.
- **Lawfully transferred outside the European Economic Area**: ASW will only transfer personal data outside the European Economic Area where the relevant agreement with this supplier is in place to accommodate all the safeguards imposed by the data protection applicable legal provisions.
- **Lawfully transferred to third parties:** ASW shall transfer personal data to a third-party controller to the extent when the legal basis exists for such a transfer. Transfer to a Third party must be in accordance

with the respective legal and regulatory requirements.

Data transfer is always allowed in the following situations:

- When the data subject has given his consent unambiguously to the proposed transfer;
- When the transfer is necessary for the performance of a contract to which the data subject is a party.
- When the transfer is necessary or legally required on important public interest grounds, such as national defense, public order or national security, for the purposes of criminal procedures or for the establishment, exercise or defense of legal claims, provided that the data to be processed is in connection with this purpose and are retained for no longer than necessary.
- When the transfer is necessary in order to protect the vital interests of the Data subject (incl. life, physical integrity or health).
- When the transfer is a result of a previous request for access to official documents that are public or a request for information that can be obtained from registers or any other publicly available documents.
- When a transfer is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party.

Both the ASW and any data processor authorized by ASW, shall keep the confidentiality of the personal data, under the requirements of the law, will not disclose, publish or otherwise reveal any information relating to personal data and operations performed without an appropriate legal basis allowing them to do so. Furthermore, data processors authorized by ASW shall disclose personal data only with the ASW's authorization, unless a legal obligation imposes data processors to act otherwise.

Accountability

ASW will implement appropriate policies and procedures as articulated in this document to demonstrate that data is processed in line with the principles set out in the GDPR.

ASW will provide comprehensive, clear and transparent privacy policies, also contained herein.

ASW will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organizational measures which demonstrate how ASW has considered and integrated data protection into processing activities. Additional internal records of ASW processing activities will be maintained and kept up-to-date by the different departments in the ASW Data Map. Internal records of processing activities will include the following:

- Name and details of the organizational unit.
- Purpose(s) of the processing.
- Description of the categories of individuals and of the categories of personal data.

- Retention schedules.
- Categories of recipients of personal data.
- Description of technical and organizational security measures.
- Details of transfers to the third countries, including documentation of the transfer mechanism safeguards in place.
- Legal basis for processing.

ASW will implement measures that meet the principles of data protection by design such as:

- Data minimization.
- Pseudonymisation.
- Transparency.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy. DPIAs will allow ASW to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to School reputation which might otherwise occur.

A DPIA will be used where a type of processing in particular using new technologies, is likely to result in a high risk to the rights and freedoms of individuals.

ASW will ensure that all DPIAs include at least the following information:

- A description of the processing operations and purposes.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An outline of the risks to individuals.
- The measures implemented in order to address risk.

Where a DPIA indicates high-risk data processing, ASW will consult the Polish Data Protection Authority to seek its opinion as to whether the processing operation complies with the GDPR.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory

authority will be informed within 72 hours of ASW becoming aware of it.

When a breach is likely to result in a high risk to the rights and freedoms of individuals, ASW shall communicate the breach to the individuals without undue delay.

The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority or individuals, will be assessed on a case-by-case basis.

Effective and robust breach detection, investigation and internal reporting procedures are in place at ASW, which facilitate decision-making in relation to whether the relevant supervisory authority or the individuals need to be notified.

Special categories data processing

Special categories of personal data (sensitive data) will only be processed under one of the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Polish law.
- The processing relates to personal data which are manifestly made public by the Data subject.
- Processing is necessary for:
    - Carrying out obligations and exercising specific rights of ASW or employee under employment, social security or social protection law, a collective agreement and child protection requirements.
    - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
    - The establishment, exercise or defense of legal claims or where courts are acting in their judicial capacity.
    - Reasons for the substantial public interest on the basis of EU or Polish law which is proportionate to the aim pursued and which contains appropriate safeguards.
    - The purposes of preventive or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of EU or Polish law or a contract with a health professional.
    - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices. See Appendix...
    - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89 (1) GDPR.

Consent

Consent must be:

- **Freely given** and should reflect the data subject's genuine and free choice without any element of compulsion, or undue pressure put upon the data subject, avoiding any negative consequences in the case of refusal to give it.
- **Specific**: ASW must clearly and precisely explain the scope and consequences of data processing.
- **Informed**: the nature of the processing should be explained in an intelligible and easily accessible form, using clear and plain language which does not contain unfair terms. The data subject should be aware at least of the identity of the controller and the purposes for which the personal data will be processed.
- **Explicit in a positive indication**: ASW will consider written declarations, email responses, and active checkboxes. Consent can not be inferred from silence, inactivity or pre-ticked boxes.

Where consent is given, a record will be kept documenting how and when consent was given.

The consent of parents will be sought prior to the processing of a student's data, except where the processing is related to preventative or services offered directly to a student.

Direct marketing

ASW shall engage in unsolicited commercial communication (direct marketing communication) only with the prior consent of the individual ("opt-in"). In every direct marketing communication that is made to the individual, the individual shall be offered the opportunity to withdraw his or her consent for further direct marketing communication. Personal data collected by ASW will never be disclosed to a Third-party company who intends to use it for direct marketing purposes unless specific consent has been given by a data subject.

Withdrawal of a consent to direct marketing

If an individual withdraws his or her consent to receive such materials, ASW will refrain from sending further marketing materials as specifically requested by the individual. ASW will do so within the time period required by applicable law. A statement of consent withdrawal should be forwarded to ASW at dpo@aswarsaw.org. Additionally, ASW keeps records to demonstrate that valid consent has been given and that the data subject has been informed.

Withdrawal of consent to processing personal data

The data subject shall have the right to withdraw his or her consent to processing personal data at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. A statement of consent withdrawal will be forwarded in the electronic form to ASW at dpo@aswarsaw.org

Data subject rights

Right to be informed

ASW will provide a privacy notice supplied to individuals in regards to the processing of their personal data and it will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

If services are offered directly to the student, ASW will ensure that the privacy notice is written in a clear, plain manner that the student will understand.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller, and where applicable, the controller's representative and the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party, where applicable.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place, where applicable.
- The retention period or criteria used to determine the retention period.
- The existence of the data subject's rights.
- The existence of the right to withdraw consent at any time (without affecting the lawfulness of processing based on consent before its withdrawal), where the processing is based on consent.
- The existence of the right to lodge a complaint with a supervisory authority.
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.
- When data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.

When data is not obtained directly from the data subject, information regarding the source the personal data originates from and whether it came from publicly accessible sources, will be provided. In such cases, the following information will also be provided:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

ASW will not provide information about processing where they reasonably consider that to do so would prejudice:

- The prevention, investigation, detection or prosecution of breaches of professional ethics or criminal offenses.
- The material rights and freedoms of any person.

Please refer to the Appendix section, for more details on privacy notices supplied to individuals in regards to the processing of their personal data.

Right of access

Individuals have the right to obtain confirmation as to whether or not that their data is being processed.

Individuals have the right to submit a Subject Access Request (SAR) to gain access to their personal data.

ASW will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge; however, ASW may impose a 'reasonable fee' to comply with requests for further copies of the same information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format, unless otherwise requested by the data subject.

Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee might be charged.

All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, within one month of receipt.

In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, ASW holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

Right to rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified.

Where the personal data in question has been disclosed to third parties, ASW will inform them of the rectification where possible.

Where appropriate, ASW will inform the individual about the third parties that the data has been disclosed to.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

Where no action is being taken in response to a request for rectification, ASW will explain the reason for this to the individual and will inform them of their right to complain to the supervisory authority and to a judicial

remedy.

Right to erasure

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws their consent, on which the processing is based, and where there is no other legal ground for the processing.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed.
- The personal data is required to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to the student.

ASW has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right to freedom of expression and information.
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- For public health purposes in the public interest.
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes.
- The exercise or defense of legal claims.

As the student may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where the student has given consent to processing and they later request the erasure of the data, regardless of age at the time of the request.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public, ASW, taking account of available technology and the cost of implementation will take reasonable steps to inform other controllers who process the personal data that the

data subject has requested the erasure by such controllers of any links to and copies of the personal data in question.

Right to restrict processing

Individuals have the right to block or suppress the schools processing of personal data.

In the event that processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

ASW will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until ASW has verified the accuracy of the data.
- Where an individual has objected to the processing and ASW is considering whether their legitimate grounds override those of the individual.
- Where the processing is unlawful and the individual opposes erasure and requests restriction instead.
- Where ASW no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

If the personal data in question has been disclosed to third parties, ASW will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

ASW will inform individuals when a restriction on processing has been lifted.

Right to data portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller.
- Where the processing is based on the individual's consent or for the performance of a contract.
- When processing is carried out by automated means.

Personal data will be provided in a structured, commonly used and machine-readable form.

ASW will provide the information free of charge.

Where feasible, data will be transmitted directly to another organization at the request of the individual.

ASW is not required to adopt or maintain processing systems which are technically compatible with other organizations.

In the event that the personal data concerns more than one individual, ASW will consider whether providing the information would prejudice the rights of any other individual.

ASW will respond to any requests for portability within one month.

Where the request is complex, or a number of requests have been received, the time frame can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, ASW will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

Right to object

ASW will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest.
- Direct marketing.
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- ASW will stop processing the individual's personal data unless the processing is for the establishment, exercise or defense of legal claims, or, where ASW can demonstrate compelling legitimate grounds for the processing, which override the interests, rights, and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

- ASW will stop processing personal data for direct marketing purposes as soon as an objection is received.
- ASW cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, ASW is not required to comply with an objection to the processing of the data.

Where the processing activity is outlined above but is carried out online, ASW will offer a method for individuals

to object online.

General provisions regarding data subject rights requests

Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee might be charged.

All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, within one month of receipt.

In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, ASW holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

Data Security

Personal data must be processed and stored in any support (electronic or paper) in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Printed data:

- Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.
- Confidential paper records will not be left unattended or in clear view anywhere with general access.

Electronic data:

- Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.
- Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.
- Memory sticks will not be used to hold personal information unless they are password- protected and fully encrypted.
- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Best practices:

- Data will be held in few places as necessary. Staff should not create any unnecessary additional datasets.

- Where possible, ASW enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- Employees will not use their personal laptops, computers or mobile devices for ASW purposes.
- All employees are provided with their own secure login and password which will be regularly changed.
    - Employees must use strong passwords. Passwords must be kept confidential and changed regularly.
- Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.
- Before sharing data, all staff members will ensure:
    - They are allowed to share it.
    - That adequate security is in place to protect it.
    - Who will receive the data has been outlined in a privacy notice.
- Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of ASW containing sensitive information are supervised at all times.
- The physical security of ASW buildings and storage systems and access to them is reviewed on a termly basis If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.
- Personal data should not be disclosed to unauthorized people, either within ASW or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their department manager or the Data Protection Officer if they are unsure about any aspect of data protection.
- User should not circumvent computer security or gain access to a system for which they have no authorization.
- Servers and workstations will be protected by using security software and implementing firewall rules. They will also be located in places specially equipped with access control and environmental controls, inaccessible to unauthorized persons.
- Data must be frequently backed up and these copies must be periodically tested to ensure data recovery.
- The access to IT systems (to personal data) will be granted by the IT department under the HR department request based on privileges required to perform their duties.
    - When access to confidential information is required, employees can request it from their department managers.
- Access controls are implemented as required, to monitor and restrict access for individuals to areas to which access is required for business purposes. These restrictions are applied as required to ASW employees, including contractors, visitors and other relevant identified third parties.
- ASW will establish retention or disposal schedules for specific categories of records in order to ensure legal compliance, and also accomplish other objectives, such as preserving intellectual property and cost management.

ASW will provide training to all employees to help them understand their responsibilities when handling data and to implement this Policy.

Responsibilities

Any person authorized by ASW and ASW's employees that are involved in the processing of personal data of data subjects or who have access to personal data in any way are required to comply with this policy.

Any ASW employee has responsibilities in terms of collecting, using and storing personal data properly. All ASW employees will read and sign the "Information Clause for Employees."

At the same time, the departments and teams are responsible for developing their own operational **procedures** to ensure that in terms of personal data the good practices are established and respected.

It is also the responsibility of each employee to inform the DPO if any change occurs with respect to the personal data.

Data Protection Officer

- Informs and advises ASW and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitors the school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.
- Reports to the highest level of management at ASW, which is the School Director and Board of Trustees.
- Handles Subject Access Requests.
- Checks and approves any contracts or agreements with third parties that may contain special categories of personal data.
- Has control and monitoring powers (the right to perform internal investigations and to access information).
- Has expert knowledge of data protection law and practices.
- Is able to operate independently without conflict of interests with its other professional duties.

Data Protection Committee

- Advises and supports Data Protection Officer in order to ensure school's compliance with the GDPR and other laws.
- Provides input and guides initiatives in order to ensure that personal data is being processed in a clear and consistent way and in compliance with the ASW internal policies and procedures;

Employees with access to personal data

- Only access personal data to the extent necessary to serve the applicable legitimate purposes for which ASW processes personal data and to perform their job.
- Report of any (possible) incident or issue relating to personal data to their manager or to the DPO.
- Never discuss confidential information in public areas or with individuals who don't have a need to know.
- Dispose of sensitive documents properly and log the disposal.

- computing devices should be powered off when not in use for extended periods of time (such as after work, on weekends, during holidays and so on).
- Lock and secure all personal data information and equipment when they are away from their desk areas.
- Keep their desk areas organized and keep all confidential information secured and out of view when away from their desks.
- Never share passwords.
- Never store passwords in plain text.
- Promptly report any suspected breach of the security policy that comes to their knowledge.
- Consult the DPO and/or the direct manager whenever they have concerns regarding data privacy.
- Have a signed authorization to process personal data on file with HR.

Director

- Ensures that an adequate organizational structure is in place as well as effective communication and reporting channels, in order to ensure that personal data is being processed in a clear and consistent way and in compliance with the ASW internal policies and procedures;
- Works together with and facilitate the appropriate DPO to create and maintain a framework for the development, implementation, and updating of local data protection policies and procedures (including training and education);
- Ensures approval and periodic review, at least yearly, of this Policy and other data protection related policies based on the proposals submitted by the responsible divisions.

Curriculum/Grade Level Leaders/Head of Departments/Managers

- Ensure that their Departments process personal data in accordance with this policy.
- Ensure that ASW staff in their organizational units is informed with regard to policies and procedures relevant to the protection of personal data.
- Ensure that personal data are processed in accordance with procedures and policies relevant to the protection of personal data.
- Notify the DPO and follow his/her advice on emerging risks or incidents.
- Ensure that the data inventory process is correct, complete and that the inventory of personal data is periodically updated.
- Ensure that the staff working in his/her department follow the required training.

Director of ICT

- Ensures that all systems, services, and equipment used for storing data meet acceptable security standards.
- Performs regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluates any third-party services (such as cloud computing services, for example) the school is considering using to store or process data in order to ensure the integrity, confidentiality, and availability of processed data.
- Identifies and implements technical measures to ensure the security of personal data stored.

- Provides support for investigating potential breaches of security.
- Provides personnel training on technical and security standards for the processing and protection of personal data.

Director of Communications and Marketing

- Ensures that the marketing strategies comply with the principles of this policy.
- Ensures that personal data database used for marketing purposes is accurate and up to date;
- Works with other ASW representatives to ensure that marketing initiatives respect the principles of personal data protection;
- Coordinates any requests of media regarding the protection of personal data;
- Endorses any statement of personal data that accompanies advertising material, or is used in communication channels (email, letters).

Director of Human Resources

- Identifies the training and development needs of the staff in connection with the processing and protection of personal data.
- Ensures the inclusion of the training materials on personal data protection within the yearly training plan.
- Ensures support to the business units for implementing the training programs regarding personal data processing and protection.
- Ensures that any action taken with regard to employee data is in line with the requirements of the Regulation. This applies to all processes managed by the human resources team, starting with the recruitment process, implementation of the employment contract and to its termination.

In all these cases, the Director of Human Resources must be involved in the decision-making process and in assessing the impact of potential projects on the protection of employees' data. The Director of Human Resources must ensure a balance between the interests of ASW and the right to the privacy of employees.

Publication of information

ASW will make available the policies and procedures regarding personal data protection and information handling.

ASW will not publish any personal information, including photos, on its website without the permission of the affected individual.

CCTV and Photography

ASW understands that recording images of identifiable individuals constitute processing personal information, so it is done in line with data protection principles. The management, operation, and use of the Closed Circuit Television (CCTV) at ASW are specified in the ASW CCTV Policy, in the Appendix 1.

Photographs and videos may be taken throughout the school year by staff, students and third-party contractors to record school life at ASW. The School may use photographic images and videos within the school for:

- Educational and informational purposes (such as keeping records of lessons, field trips, sports, events, staff training).
- Marketing and publication purposes, if and to the extent, we have obtained the parent's and/or student's consent where required under applicable data protection legislation to do so
- Identification and official purposes (such as student information, school ID card, diploma/report cards or other official documents).
- Yearbook.

Please refer to our Photography and Video Policy for more details on how we use these images.

Photographs and videos captured by ASW parents for personal consumption are exempt from the GDPR.

Policy review

This policy is reviewed yearly by the DP Committee and the School Director.

The next scheduled review date for this policy is June 2021

Appendix 1 - CCTV Guidelines

Introduction

The American School of Warsaw (ASW) uses CCTV in alignment with General Data Protection Regulation (GDPR - EU 2016/6790), the school Data Protection Policy, and Art. 108a of the Polish Law on Education. The American School of Warsaw holds the responsibility of the data obtained with CCTV as the Data controller.

ASW has a CCTV camera system in place to monitor the school grounds, its students, staff, and visitors. All cameras are monitored under restricted access from the two security offices and receptions. The CCTV system is owned by the school and no outside parties can view the images.

Statement of Intent

Cameras are used to control access points, corridors, and playgrounds, all for the purpose of securing the safety of the school's students, staff and visitors.

The footage is used to detect, record and hopefully resolve potential illegal or dangerous situations. The recorded material will not be used for any commercial purpose and the recordings will be deleted on a monthly basis. Recordings will never be released to the media or for the purpose of entertainment.

The planning and design have endeavored to ensure that the cameras will give maximum effectiveness and efficiency. However, it is not possible to guarantee that the system will detect every incident taking place in the areas of coverage.

Cameras are used to monitor activities within the school and to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety of students and staff, and property protection of the school, together with its visitors.

CCTV Surveillance signs have been placed at all access routes to the ASW campus.

System Management

The system is administered by the Head of Security in accordance with the principles and objectives expressed in the policy. The system and the data collected is only available to the ASW Security Supervisors, Head of Security, and School Director.

The CCTV system is operated 24 hours a day, every day of the year. The Head of Security will check and confirm the efficiency of the system daily and, in particular, that the equipment is properly recording and that cameras are functional.

Law enforcement will have access to recorded material in case of an investigation.

Location of Cameras

The cameras are located at strategic points all throughout the school. Monitoring does not include rooms in which didactic, educational and caring classes take place, rooms in which psychological and pedagogical help is given to students, staff lounges, sanitary and hygienic rooms, nurse's office, and changing rooms, unless the use of monitoring in these rooms is necessary due to the existing security or safety threat and it will not violate the students' and staff 's dignity and other personal rights.

Image storing and access to CCTV

Images are recorded in real time 24 hours a day. Recorded images are stored for one month before being deleted. However, if law enforcement is investigating a crime, images may be retained for a longer period.

Downloaded media required as evidence will be properly recorded and packaged before copies are released to the police.

ASW Security can view the live images but only the ASW Head of Security and Security Supervisors have access to the recordings and settings.

Public Information

ASW CCTV Policy will be available at the Security Desk in the Main Building, Head of Security's Office, and on the ASW website. The students and the staff will be informed about the use of monitoring by the school in the manner prescribed by law.

Complaints

Any complaints regarding the school's CCTV system should be addressed to the School Director or the Data Protection Officer at dpo@aswarsaw.org.

Summary of Key Points

The CCTV system is owned and operated by ASW.
The CCTV system and images are not available to the public under any circumstances.
Liaison meetings may be held with the police and other involved bodies if required.
Downloaded media will be used properly: indexed, stored and destroyed after appropriate use, in accordance with the GDPR. Images may only be viewed by authorized school personnel and law enforcement.

Subject Access Request

In alignment with Article 15 (1) of GDPR as well as the ASW Data Protection Policy (Right of Access), individuals have the right to submit a subject access request (SAR) to gain access to their CCTV personal data in order to verify the lawfulness of the processing.

To request access to CCTV information that ASW holds about your son/daughter, please contact dpo@aswarsaw.org.

Appendix 2 - Privacy Notice - Visitors

Your data is held and processed in accordance with the General Data Protection Regulation (GDPR) and the ASW Data Protection Policy available at the following website: https://www.aswarsaw.org/about-us/policies.

In order to provide a safe and secure learning environment, we obtain basic personal information from our Visitors upon arrival. The data is kept in the Visitor logbook and includes the name license plate number, date of visit, and the point of contact at ASW. Video footage is also being recorded on our CCTV system installed on the premises.

ASW is committed to keeping your personal data in a secure manner. Only authorized employees and security personnel has access to them.

CCTV footages are stored for 30 days and visitor log books for 2 academic years before being deleted.

ASW does NOT transfer or share your personal data with other persons or organizations unless required by law.

Under the GDPR, you have a right to access, rectify, erase, object to certain processing of your data. Should you wish to exercise them, or if you have any concerns as to how your data is processed please contact our Data Protection Officer at dpo@aswarsaw.org.

Appendix 3 - Privacy Notice - Parents/Students

The American School of Warsaw with its registered office in Bielawa, ul. Warszawska 202, 05-520 Konstancin-Jeziorna, Poland (ASW) processes personal data on its prospective, current and former students and their parents or legal representatives, as part of its everyday operations of providing educational services.

ASW handles your personal data according to the General Data Protection Regulation no. 679 / 2016 (GDPR) and the school Data Protection Policy. For these purposes, ASW acts as a controller with regard to your personal data and the personal data of students, meaning ASW establishes the purposes and means of personal data processing.

This notice is to help you understand how and why ASW collects your personal information and what we do with that information. It also explains the decisions that you can make about your own information. If you have any questions about this notice please contact our Data Protection Officer at dpo@aswarsaw.org.

What is personal data?

Personal data is any information that identifies you and/or the students – directly or indirectly – as an individual. This includes information such as name, date of birth, student ID, contact details, billing information, academic records, teacher references, attendance information, photographs, etc. ("Personal Data").

What does data processing mean?

For the purposes of this Privacy Notice, please note that when we refer to data processing we refer to any operation or set of operations which is performed on personal data, either by automated or manual 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.

Which are the purposes for which ASW processes your Personal Data?

ASW processes Personal Data that pertain to you or to the students for the following purposes:

- **Provision of educational services**, starting with the application process, enrolling students, administration of classes and timetable, teaching activities, administration of internal and public examinations, assistance regarding the application process to various universities, issuance of academic records.
- **Provision of educational ancillary services**: career and personal counseling, library services, extracurricular activities, school trips, managing the school's publications, setting up the virtual learning environment and granting access to ASW's Intranet and Internet network as well as monitoring the use of ASW's network.
- **Ensuring campus security**: monitoring access on campus, the performance of video surveillance.
- Provision of medical **care and counseling** that students may need.

- **School administration**: handling student records and other academic documentation, administration of fees and accounts, internal audits and controls, reporting and statistics creation, implementing school policies, ensuring collaboration with other schools, archiving, assessing the quality of our services, facilitating research activities.

- **School-related communications**: conveying various messages related to the students and ASW's activities by any communication means.

- Organizing **fundraising activities** and **other school events** (e.g., concerts, theatre productions, shows, tournaments, fairs), including marketing communications related to the activities organized by ASW.

- Dispute resolution and litigations.

Which categories of Personal Data does ASW process?

The categories of Personal Data that ASW processes include, but are not limited to the following:

- Identification and contact information (first and last name, citizenship, country of birth, address, information included in IDs/passports, phone number, email, etc.).

- Payer information (billing address, name of the payer, payer email address)

- Health data: medical history, allergies, immunization records, medical examination results and other medical data of the students.

- Medical Insurance details.

- Emergency contact information.

- Data related to the educational background and regarding school performance of the students: academic, disciplinary or other educational related records, academic references, special needs, hobbies, results of educational diagnosis testing, test results, feedbacks, evaluations etc.

- Behavioral data as well as data on students.

- Family information: household information, student custody, language background, profession and workplace of parents, etc.

- Authentication and physical access data: email, passwords, badge number, location data, other online identifiers, car details, etc.

- Image (photographs and videos).

Generally, the Personal Data held by ASW is provided directly by the parents or results from the interaction that the parents and the students have with the school. In some cases, third parties (e.g., representatives of former schools and/or outside referral centers attended by students) may supply some data.

Which is the lawful basis for the processing operations ASW conducts with regard to the Personal Data?

ASW collects and further processes Personal Data, based on one of the following legal grounds, expressly laid down by the GDPR:

- The **consent** you have granted us, prior to any processing of personal data, for:
    - Evaluation of the student for admission to the school
        - There are some mandatory categories of personal data necessary to ASW in order to evaluate the student for admission, make an offer of enrolment and provide the educational services to students at a high standard and in the best interest of the students. The mandatory categories of personal data are included and marked accordingly in the application form. All the mandatory categories of data are necessary for ASW to be able to evaluate your application and finally to enroll the student. Failure to provide all the information marked as mandatory will lead to the impossibility of ASW to process your application.
    - The use of students' photographs and videos in various school publications, on ASW's website and social media pages.
    - The use of your contact details for direct marketing communications or fundraising activities.
    - Other consents that may be granted from time to time for various processing activities.
- For providing the educational services in execution of **the enrolment contract** or in order to take steps prior to entering into the enrolment contract.
- A **legal obligation** that requires ASW to process your Personal Data. For example, AW may disclose your information to third parties such as the courts, the local authority or the police where legally obliged to do so.
- The **legitimate interest pursued by ASW**.

ASW relies on this legal ground in order to provide the educational services it has committed to deliver and additional services related to this scope at the highest standards, always for the benefit of the students and without outweighing the parents or the students' rights and liberties.

ASW may invoke the legitimate interest legal ground in the following cases:

- Issuing and storing academic records, evaluating students' performance, etc.
- Monitoring use of the ASW's virtual learning environment and network, including monitoring the use of e-mail accounts provided by ASW.

- Conducting and marketing fundraising activities and other school-related events.
- Enforcement of legal claims, addressing complaints and third-party controls.
- Management, control, reporting and performing statistics on schools activity.
- Ensuring security.
- Maintaining close relationships with alumni and ASW's community.
- Collaboration with other schools and educational institutions.
- Performance of agreements with suppliers, including insurance suppliers.
- Access to grants and other funding sources.

With respect to the processing of the **special categories of personal data under the GDPR**, respectively health data of students, please take into consideration that ASW processes **health data** based on the following legal grounds:

- Processing is necessary during the admissions process to evaluate whether the student's medical needs can be met at ASW.
- Processing by the Nurse's Office is necessary during enrolment to promote student health and safety, provide interventions, early identification of problems, and referrals. The necessity of the Nurses' Office to process such data for the purpose of preventive and occupational medicine, medical diagnosis and the provision of health or social care or treatment on the basis of European Union or national law.
- Processing is necessary for reasons of substantial public interest, on the basis of the European Union or Polish law. Such a legal ground is used especially in those situations where the school has to assess the learning capacity of a student and adapt the teaching activities to the special needs of a student.
- The explicit consent granted by you for the disclosure of the personal data of students related to the allergies they suffer from or any other medical alerts.

Does ASW disclose Personal Data?

ASW discloses your Personal Data only to those members of ASW, staff, and collaborators, who need access to the personal data mainly for ensuring the provision of the educational and ancillary services. In this respect, please take into account that only the Nurses' Office has access to the students' medical records.

Other departments of the school have access to specific health data based on the consent you have expressed (i.e. for allergies) or in order to protect a substantial public interest based on European Union or Polish law (e.g., various medical conditions triggering special learning needs).

With respect to the disclosure of your Personal Data to third parties, outside ASW, please note that such disclosure is performed solely in the regular activity of the school. The categories of recipients include the following:

- IT providers, including educational applications, online tools, server hosting suppliers such as OpenApply, CHQ, Google Suite, NWEA, WIDA and College Board, etc.
- The catering company in its capacity of an independent provider of meal services on campus.
- Other educational institutions or organizations, not limited to other schools.
- Travel agencies, catering and transportation providers,
- Photographers and videographers.
- Courier services providers.
- Public authorities and institutions, national or foreign, judicial courts and foreign embassies or other forms of diplomatic missions.
- Tax, legal and accounting consultants/auditors.

Third country transfers

The School may transfer your personal data to recipients in the United States, Canada, Japan, Malaysia, Taiwan, Hong Kong, India [...], [...], [...]., especially IT providers, including educational applications, online tools, server hosting suppliers or other educational institutions or organizations, not limited to other schools.

Personal data is transferred outside the EU only on the basis of a European Commission adequacy decision, the EU Model Clauses or on the basis of a derogation provided for in art. 49 GDPR (when the data is transferred to the United States). In such cases the school will do everything that is required to assure safe processing of data by entities from such countries, in accordance with the provisions of law. Educational resources are screened for compliance, running record of educational resources where international data transfer occurs is kept and updated on the ongoing basis.

If you wish to consult the appropriate safeguards put in place by ASW regarding the transfer of personal data to other countries, please refer to the contact point at the end of this Privacy Notice.

For how long does ASW retain your Personal Data?

ASW holds all your Personal Data for as long as you are in a contractual relationship with us, and afterward for a standard period of 6-years, for which ASW can justify a need in storing such personal data. ASW keeps the student file and all the data related to the student interaction with ASW mainly for the scope of assessing the school's activity and the quality of services provided but also for addressing potential request of students with regard to their school trajectory within ASW, which usually appear after the students have graduated or transferred to another school. Moreover, ASW takes into account also standard limitation period of the claims.

Notwithstanding the retention period mentioned above, please be informed that all the academic records and other school acts and documents related to study activities are kept for an indefinite period of time, according to the legal obligations that ASW has in this respect. Moreover, in any case, where a legal provision imposes a minimum retention period, ASW will keep the Personal Data for at least that mandatory period.

For inquiries and declined applications, your personal data will be processed for the period of the application process, and maximally for 1 year from the end of the calendar year when the application process was completed (for the purposes of defense against potential claims).

Which are your rights related to the processing of Personal Data by ASW?

The GDPR provides certain rights related to the processing of personal data, that both you and the students have. In this respect, please be informed that students that are 18 years or above could exercise the rights listed in this section, individually.

ASW respects all the rights mentioned under the GDPR and is committed to furnishing the appropriate means by which you can exercise these rights, according to the details mentioned below:

- The **right of access**, which entails your possibility to obtain the confirmation from ASW whether your Personal Data is being processed by ASW or not, and if the case may be you are entitled to solicit access to this data, as well as additional information regarding the Personal Data, such as the purposes of processing, the categories of recipients the Personal Data are being disclosed to and the envisaged retention period. The right of access also includes a right to obtain a copy of the personal data undergoing processing. In the situations where you may need to exercise the right of access, please consider contacting ASW and requesting confirmation by e-mail at dpo@aswarsaw.org. Please consider that there might be specific situations that are exempted from the right of access, such as information that identifies other individuals or which is subject to confidentiality obligations.
- The **right to rectification**, that allows you to request ASW to rectify any inaccurate Personal Data that ASW may hold, as well as to have your incomplete Personal Data completed.
- The **right to erasure** meaning that in the situations expressly regulated by law, you may request the erasure of your personal data. Please take into account, that the cases where the law provides for the possibility of erasure of personal data amount to the situations where i.a. the processing is unlawful or where the processing is based on your consent, and you have withdrawn such consent.
- The **right to restriction of processing**, signifying your right to obtain restriction of processing your Personal Data from ASW's part. Please bear in mind that this right can be exercised only in specific situations laid down by the GDPR such as when you challenge the accuracy of your Personal Data. During the period necessary for us to rectify your data, you may ask us to restrict the processing of your Personal Data.
- The **right to data portability** implying your right to receive the personal data in a structured, commonly used and machine-readable format and further to transmit such data to another controller. This right to data portability shall be applicable only to the personal data you have provided to us and where the processing is carried out by automated means based on your consent or for the performance of the contract you have concluded with ASW.
- The **right to object** to the processing of your Personal Data by ASW, on grounds relating to your particular situation. The right to object applies to the situations where ASW relies on the legitimate interest pursued by the School (e.g. using your email address for conveying fundraising related messages).

- The **right to lodge a complaint** designates your right to challenge the manner in which ASW performs processing of your Personal Data with the competent data protection authority.

If you believe that the School processes personal data in breach of personal data protection provisions, you have the right to submit a complaint to the President of the Personal Data Protection Office. The Personal Data Protection Office is located in Warsaw (00-193) ul. Stawki 2, tel. 22 531 03 00, website and electronic inbox: https://uodo.gov.pl

- The **right to withdraw your consen**t given for various processing operations, in cases where the consent represents the lawful basis for processing. In cases where you withdraw your consent to processing your Personal Data, please note that the processing will end from the moment the withdrawal takes place without any effect on the processing that took place prior to such withdrawal.

Profiling

ASW creates various profiles through automated means based on the Personal Data that pertain to students. Generally, such profiles are created via various applications used in the online education environment such as MAP Testing Tool and NWEA.

ASW creates and uses such profiles to evaluate the performance of its students, to identify gaps in their development or to assess specific traits that characterize students' personality, preferences, and behavior or professional inclinations.

Based on such profiles ASW, however, will not make with respect to the student any automated decisions, which produces legal effects concerning him or her or similarly significantly affects him or her.

CCTV Surveillance

ASW uses video surveillance system (CCTV) on the campus, in order to ensure the security of its students, staff and all other persons that enter our premises. The security and wellbeing of our students is our primary concern and these video cameras allow us to offer real-time protection. The legal basis for such monitoring is Art. 108a of the Polish Education Law (Act of 14 December 2016) in connection with Art. 6(1)(f) of GDPR.

All the areas covered by a video camera are identified on campus through specific banners, informing you of the video surveillance conducted by ASW.

Video surveillance recordings may be disclosed to third parties such as the police and will be kept for 30 days.

Photographs and Videos

The photographs and videos may be taken throughout the school year by staff, students and third-party contractors to record school life at ASW. The School may use photographic images and videos within the school for:

- Educational and informational purposes (such as keeping records of lessons, field trips, sports, events, staff training).
- Marketing and publication purposes, if and to the extent, we have obtained you and/or your child's consent where required under applicable data protection legislation to do so

- Identification and official purposes (such as student information, school ID card, diploma/report cards, and other official documents)
- Yearbook.

We will not publish photographs or video of individuals alongside their names publically or in school publications, Newsletters, Social Media Sites or on the school website, unless we have obtained your and/or the student's explicit consent.

Contact Point

In a situation where you may wish to exercise any of the rights listed in this Privacy Notice or to obtain additional information or clarification on the subject of processing your Personal Data please contact ASW via its appointed Data Protection Officer, who is responsible for ensuring that ASW complies with all the requirements of the GDPR.

Contact Details of ASW Data Protection Officer

E-mail address: dpo@aswarsaw.org

The present Privacy Notice shall apply along with the ASW Data Protection Policy.

Appendix 4 - Privacy Notice - Employees

The American School of Warsaw (ASW) processes employee personal data as part of its everyday operations of providing educational services.

ASW handles your personal data according to the General Data Protection Regulation no. 679 / 2016 applicable in the European Union (GDPR) and the school Data Protection Policy. For these purposes, ASW acts as a controller with regard to your personal data, meaning ASW determines the purposes and means of the processing of the Personal Data, being responsible for the safe and lawful use of your data.

This notice is to help you understand how and why ASW collects your personal information and what we do with that information. It also explains the decisions that you can make about your own information. If you have any questions about this notice please contact dpo@aswarsaw.org.

Definitions

For the purpose of this Privacy Notice, please consider that the terms listed below shall have the following meaning.

Personal Data	is any information that identifies you – directly or indirectly – as an individual. This includes information such as name, date of birth, ID, contact details, references, attendance information, photographs, etc.
Data Processing	any operation or set of operations which is performed on personal data, either by automated or manual 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.

What are the purposes for which ASW processes your Personal Data?

ASW processes Personal Data that pertain to the employees for the following purposes:

- Concluding employment contracts, as the case may be and performance of such contracts.
- Providing visa, obtaining related support to overseas employees and dependents.
- Providing support as regards to opening a bank account at a Polish bank as well as support regarding the relocation to Poland for the duration of the contract.
- For human resources purposes as well as in order to carry out the employer's obligations resulting from specific provisions: including those connected with compulsory social and health benefits, tax authorities (local hires), personnel evaluation, professional development, disciplinary procedures,

payroll activities, handling personnel registers and files, ensure health and security at work and complying with all the legal obligations related to the employment field;

- For verification of the possibility to engage you in work with the School's students and for the purpose of assuring safety at the place of work based.
- To assure the organization of work enabling full use of the working hours, and proper use by the employee of the work tools, by means of monitoring of your electronic mail and data downloaded to the work tools entrusted to you, such as business mobile phone, tablet or laptop computer, etc.
- Providing educational services that represent the core activity of ASW, such as teaching activities, student assessment, counseling, organizing school trips, management of school's publications, organizing international examinations;
- **Provision of educational ancillary services**: career and personal counseling, library services, extracurricular activities, school trips, managing the school's publications, setting up the virtual learning environment and granting access to ASW's Intranet and Internet network as well as monitoring the use of ASW's network.
- **Ensuring campus security** (to assure the safety of the School's employees and students, as well as to protect property): monitoring access on campus, the performance of video surveillance.
- Provision of **medical care**.
- **School administration**: handling academic documentation, administration of accounts, internal audits, and controls, reporting and statistics creation, implementing school policies, ensuring collaboration with other schools, archiving, assessing the quality of our services, facilitating research activities.
- **School-related communications**: conveying various messages related to the students and ASW's activities by any communication means.
- Organizing **fundraising activities** and **other school events** (e.g., concerts, theatre productions, shows, tournaments, fairs), including marketing communications related to the activities organized by ASW.
- Dispute resolution and litigations.

Which categories of Personal Data does ASW process from its employees?

The categories of Personal Data that ASW processes include the following:

- Identification information: first name, last name, gender, date of birth, nationality, PESEL number, ID card or passport number, other data resulting from a scan of an ID card or passport, driving license number, photography.
- Contact information: phone number, personal e-mail address, address of residence.

- Visa/residency permit related information, first name, last name, gender, date of birth, nationality, passport number, home of record other data resulting from a scan of an ID card or passport and photography of employee and all dependents.
- Professional Information: academic degrees, teaching credentials, qualifications, relevant past experience, number of teaching years, references, feedback provided via the Search Associates platform.
- Personal Information: marital status, number of children, personal data on authorized dependents as such dependents using social or company benefits or assistance in the scope of staying and working in Poland.
- Medical insurance details.
- Retirement for overseas hires (those who are in the school's sponsored plan): first and last name, date of birth, Social Security Number, address in the United States, the balance of the accumulated contributions in the program.
- Financial data: remuneration and bank account details.
- Personal data resulting from employee interaction with the School: results concerning the course of employment and work assessment, absences from work and justifications of absences from work, training attended, position within ASW, badge number, location data, car details provided for parking purposes;
- Health data: information extracted from the Medical Report presented at the recruitment stage for overseas hires, as well as health data provided during the employment period.
- Criminal Record: data on convictions or criminal security measures/interdictions imposed as a consequence of criminal convictions. Such data are collected from the criminal record presented in the recruitment phase and periodically during employment contract as needed by school child protection policy.
- ASW's allocated email account or other online identifiers and personal data that may result from monitoring the use of the allocated e-mail account and the use of the School's Intranet and Internet network as well as the school allocated laptop.
- Photographs and videos.

Generally, the Personal Data held by ASW is received directly from employees via the application form, the Curriculum Vitae, medical reports, criminal records and all the supporting documentation provided in the recruitment and hiring process. Personal data may also be obtained by ASW during the collaboration of an employee with ASW.

However, specific categories of personal data may come from other external resources. We refer here to the following:

- References provided by former employers, after prior consent of the data subject with regard to the consultation of this former employers;
- Personal data listed on Search Associates, International School Services or TIE or other recruitment agencies – international and Polish recruiting platforms (after prior consent of the data subject);
- Personal data on professional background extracted from professional social media profiles, such as Linkedin or other professional links that may have been provided to us in the job application form (only with respect to links provided us in the job application form or after prior consent of the data subject).

All the external resources are consulted by the School with the sole purpose of assessing and verifying the professional capabilities that an applicant may have.

ASW processes personal data of dependents when an employee wishes to reallocate in Poland his/her dependents, for visa/residency permit purposes and also in order for the School to take all measures in order to accommodate the entire family, including providing the family with medical insurances and other applicable benefits.

For this situation, the employee who discloses personal data on dependents has the obligation to provide the dependents with information on the disclosure of their data to ASW and the reasons for such disclosure, and even if the case may be to present them this Privacy Notice.

Personal data of these data subjects related to an employee are handled by ASW in accordance with all data protection principles and the School ensures that the rights of these data subjects are fully complied with.

Which is the lawful basis for the processing operations ASW conducts with regard to the Personal Data?

ASW collects and further processes Personal Data, based on one of the following legal grounds, expressly laid down by the Art. 6(1) of GDPR:

- Processing is **necessary for the performance of the contract,** or in order to take steps at the request of the contractor to enter into such a contract. (Art. 6(1)(b) of GDPR)

With reference to this legal basis for processing, please note that there are certain categories of personal data, which are mandatory for entering into a contract with ASW under Art. 22^1 of the Polish Labour Code. All the mandatory categories of personal data were marked accordingly in the job application form or presented as such by the School at the recruitment phase. Failure to provide ASW with these mandatory categories of personal data will result in the impossibility to enter into or perform a contract with the School.

- The data subject has given consent to the processing of his / her personal data. (Art. 6(1)(a) of GDPR)

ASW may also process personal data other than those stipulated in the provisions of law (e.g. facial image) for human resources purposes, verification of the possibility to engage you in work with the School's students and for the purpose of assuring safety of parents, students, staff and service providers based on voluntary consent

granted by you (legal basis: Art. 6 (1)(a)). The consent granted may be revoked at any time. With respect to data that we can process based on your voluntary consent, not providing us with them or revocation of the consent does not have any adverse consequences.

- Processing is necessary for **compliance with a legal obligation** the School is subject to, such as the obligations that ASW has in the field of employment or social security. (Art. 6(1)(c) of GDPR)

We refer here to the processing activities carried out in order to organize students' official assessments and evaluations.

- Processing is necessary for the purposes of the **legitimate interest pursued by the School**, except where such interest is overridden by the interest and the fundamental rights and freedoms of data subjects. (Art. 6(1)(f) of GDPR)

The legitimate interests pursued by ASW consist of the following:

- monitoring the use of the ASW's virtual learning environment and network, school-issued computers, including monitoring the use of emails account provided by ASW;
- evaluate the performance of staff and improve the quality of the educational services rendered;
- keep records of personnel or applicants, besides the records that are mandatory by law;
- conducting fundraising activities, including marketing of such activities;
- enforcement of legal claims, addressing complaints and third-party controls;
- management, control, reporting and performing statistics on school's activity, including but not limited to teaching activities;
- ensuring security;
- maintaining close relationships with alumni and ASW's community;
- collaboration with other schools and educational institutions;
- performance of agreements with suppliers/collaborators, including insurance suppliers;
- performance of enrollment agreements and attracting future students;
- access to grants and other funding sources.

With respect to the processing of the *criminal background data and special categories of personal data*, the School relies upon the following legal basis for processing:

- ***Criminal Background data***, regarding educators and staff working in a school setting, are processed since processing of such data is necessary for compliance with a legal obligation (Art. 10 of GDPR in relation to Art. 10(8a) and Art. 91b(2b) of the Act of 26 January 1982 – The Teacher's Charter) for the purpose of verification of the possibility to engage the employee in work with School's students and to assure the student's safety.

- Data contained in the Certificate of lack of criminal record, regarding staff members other than teachers and educators, are processed based on staff member consent (legal basis: art. 6 sec. 1 a) GDPR) for the purpose of verification to determine whether you are eligible to work in an environment with students of the School and assure student safety.

- ***Health Data*** is processed for the purpose of carrying out the obligations and exercising specific rights that the School or collaborators of the School have in the field of employment and social security and social protection law insofar as authorized by Union or Polish law or a collective agreement. In addition, the processing of health data is necessary for the assessment of the working capacity of an employee. Health Data might be also processed for verification of the possibility to engage you in work with the School's students and for the purpose of assuring the safety of parents, students, staff and service providers based on voluntary consent granted by you. Health Data is therefore processed based on the provisions of law (in the scope specified in the Polish Labour Law or in the Social Security and Social Protection Law) or based on consent given by an employee (in case of filling in of the form by foreign employees) (Art. 9(2)(b) and Art. 9(2)(a) of GDPR).

With respect to data that we can process based on your voluntary consent, the consent granted may be revoked at any time and revocation of the consent does not have any adverse consequences. However, in certain situations, this may affect the assessment of your qualifications from the point of view of the School's duty to assure the safety of its students and other persons on its premises, especially described in the Child Protection policy.

Does ASW disclose Personal Data?

At various stages of the interaction between contractors/employees and ASW, personal data are disclosed to different recipients.

After ASW has decided with regard to an application, in order to take the corresponding steps for the execution of the teaching services contract, as well as afterwards for the entire duration of the said contract, ASW may disclose personal data to the following categories of recipients:

- Personal data constituting business contact details as well as data on the business ID or in the authorization granted may be shared with institutions cooperating with the School and with the parents/guardians of students.
- Data confirming professional licenses or occupational safety and hygiene and fire protection drills that the employee participated in.
- Personal data may also be shared with entities processing data on behalf of the School, participating in performance of the School's data processing activities:
    - IT providers, including educational applications, online tools, server hosting suppliers such as CHQ, OpenApply, and NWEA, etc.;
    - entities providing for the benefit of the School;
    - recruitment and training services;
    - Cafeteria in its capacity of an independent provider of meal services on campus;
    - Sponsors and other participants at ASW's fundraising events;
    - Travel agencies, catering and transportation providers;

- ASW's photographer and video crew;
- Tax, legal and accounting consultants and auditors.

- Personal data may also be shared with entities processing data on their own behalf:
  - courier or post services;
  - Bank, financial institutions and insurance providers;
  - Public authorities and institutions, including fiscal authorities and authorities in the field of social security, national or foreign, judicial courts and foreign embassies or other forms of diplomatic missions.

Third country transfers

The school may transfer your personal data to recipients in the United States, Canada, Japan, Malaysia, Taiwan, Hong Kong, India [...], [...], [...]., especially IT providers, including educational applications, online tools, server hosting suppliers or other educational institutions or organizations, not limited to other schools.

For the School's accreditation purposes as well as to assure insurance for the employees, the school may transfer data to the United States, Canada, New Zealand, and Australia.

Personal data is transferred outside the EU only on the basis of a European Commission adequacy decision, the EU Model Clauses or on the basis of a derogation provided for in art. 49 GDPR (when the data is transferred to the United States). In such cases the school will do everything that is required to assure safe processing of data by entities from such countries, in accordance with the provisions of law.

For how long does ASW retain your Personal Data?

Your personal data will be processed during the term under the Contract as well as in the scope required under the legal provisions:

- personal files and payroll information:
  - persons employed up to 31 December 2018 – for the period of 50 years from the end of the employment relationship;
  - persons employed after 1 January 2019 – for the period of 10 years from the end of the employment relationship;
- the remaining personal information – for the period of 6 years from the end of the year when the employment relationship ended;
- CCTV footage – for the period of 30 days, and in case of necessity of additional analysis – no longer than 3 months from the date of recording thereof.

It is important to mention that after a contractor terminates its collaboration with the School, his file containing personal data on him/her is declared inactive and only certain members of ASW's staff shall have access to it, based on strict justifications.

Which are your rights related to the processing of Personal Data by ASW?

The GDPR provides certain rights related to the processing of personal data. ASW respects all the rights mentioned under the GDPR and is committed to furnishing the appropriate means by which you can exercise these rights, according to the details mentioned below:

- The **right of access**, which entails your possibility to obtain the confirmation from ASW whether your Personal Data is being processed by ASW or not, and if the case may be you are entitled to solicit access to this data, as well as additional information regarding the Personal Data, such as the purposes of processing, the categories of recipients the Personal Data are being disclosed to and the envisaged retention period. In the situations where you may need to exercise the right of access, please consider contacting ASW and requesting confirmation by e-mail at dpo@aswarsaw.org. Please consider that there might be specific situations that are exempted from the right of access, such as information that identifies other individuals or which is subject to confidentiality obligations.

- The **right to rectification**, that allows you to request ASW to rectify any inaccurate Personal Data that ASW may hold, as well as to have your incomplete Personal Data completed.

- The **right to erasure** meaning that in the situations expressly regulated by law, you may request the erasure of your personal data. Please take into account, that the cases where the law provides for the possibility of erasure of personal data amount to the situations where i.a. the processing is unlawful or where the processing is based on your consent, and you have withdrawn such consent.

- The **right to restriction of processing**, signifying your right to obtain restriction of processing your Personal Data from ASW's part. Please bear in mind that this right can be exercised only in specific situations laid down by the GDPR such as when you challenge the accuracy of your Personal Data. During the period necessary for us to rectify your data, you may ask us to restrict the processing of your Personal Data.

- The **right to data portability** implying your right to receive the personal data in a structured, commonly used and machine-readable format and further to transmit such data to another controller. This right to data portability shall be applicable only to the personal data you have provided to us and where the processing is carried out by automated means based on your consent or for the performance of the contract you have concluded with ASW.

- The **right to object** to the processing of your Personal Data by ASW, on grounds relating to your particular situation. The right to object applies to the situations where ASW relies on the legitimate interest pursued by the School (e.g. using your email address for conveying fundraising related messages).

- The **right to lodge a complaint** designates your right to challenge the manner in which ASW performs processing of your Personal Data with the competent data protection authority.

- The **right to withdraw your consen**t given for various processing operations, in cases where the consent represents the lawful basis for processing. In cases where you withdraw your consent to processing your Personal Data, please note that the processing will end from the moment the withdrawal takes place without any effect on the processing that took place prior to such withdrawal.

Profiling

Based on your personal data, the School will not make with respect to you any automated decisions, including decisions resulting from profiling. Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

CCTV Surveillance

ASW uses video surveillance system (CCTV) on the campus, in order to ensure the security of its students, staff and all other persons that enter our premises. The security and wellbeing of our students is our primary concern and these video cameras allow us to offer real-time protection. The legal basis for such monitoring is Art. 22^2 of the Polish Labour Code in connection with Art. 6(1)(f) of GDPR.

All the areas covered by a video camera are identified on campus through specific banners, informing you of the video surveillance conducted by the ASW.

Video surveillance recordings may be disclosed to third parties such as the police and kept for 30 days and in case of necessity of additional analysis – no longer than 3 months from the date of recording thereof.

Photographs and Videos

The photographs and videos may be taken throughout the school year by staff, students and third-party contractors to record school life at ASW. The School may use photographic images and videos within the school for:

- Educational and informational purposes (such as keeping records of lessons, field trips, sports, events, staff training).
- Marketing and publication purposes
- Identification and official purposes (such as ID and other official documents)
- Yearbook.

In such case, ASW will process your image only under your consent (Art. 6(1)(a) of GDPR) expressed in the Contract separately.

Contact Point

In a situation where you may wish to exercise any of the rights listed in this Privacy Notice or to obtain additional information or clarification on the subject of processing your Personal Data please contact ASW, via its appointed

Data Protection Officer, who is responsible for ensuring that ASW complies with all the requirements of the GDPR.

If you believe that the School processes personal data in breach of personal data protection provisions, you have the right to submit a complaint to the President of the Personal Data Protection Office. The Personal Data Protection Office is located in Warsaw (00-193) ul. Stawki 2, tel. 22 531 03 00, website and electronic inbox: https://uodo.gov.pl

Contact Details of ASW Data Protection Officer

E-mail address: dpo@aswarsaw.org

The present Privacy Notice shall apply along with other policies/procedures adopted at the level of ASW.

Appendix 5 - Consent form - Hosted Event

Hosted Event Name

@ the American School of Warsaw

Parent/Guardian Data Processing Consent Form

Pursuant to the provision of Article 6 (1a), Article 7 (2) and Recital 32 of the European General Data Protection Regulation (GDPR 2016/679), by signing this document, I agree that my child's

- Name
- Emergency contact numbers
- Date of Birth
- Health and/or diet information

can be used by the American School of Warsaw (ASW), referred herein as "Data Controller", for **EVENT NAME** hosting purposes. Thus, my child's name can appear in the **EVENT NAME** related publications, website, and within ASW and software from third parties. I understand that the data listed above will be deleted within 21 days of the event completion date.

In addition, I hereby provide my consent to my child being interviewed, photographed or videotaped at events hosted by the **EVENT NAME**. Furthermore, I consent to the publication, exhibition or reproduction of any such interview material, photographs or videotapes to be used by ASW for news articles, live streaming, education or marketing publications, including the **EVENT NAME** and ASW social media.

I am aware of my right to withdraw my consent in writing at any time.

Student Name and Last Name:
_____

Guardian Name and Last
Name:_____

Date:_____

Signature:_____

ASW Data Protection Policy is available at https://www.aswarsaw.org/about-us/policies

Appendix 6 - GDPR Information Clause for Employees in connection with special measures during COVID-19 epidemic

Konstancin-Jeziorna, 14 August 2020

Klauzula informacyjna RODO dla pracowników w związku ze specjalnymi Środkami podejmowanymi w okresie stanu epidemii COVID-19

The American School of Warsaw z siedzibą w Bielawie, ul. Warszawska 202, 05-520 Konstancin-Jeziorna (zwana dalej „**Administratorem**" lub „**Szkołą**"), posługująca się stroną internetową www.aswarsaw.org, informuje, że:

1. Zgodnie z przepisami ogólnego rozporządzenia o ochronie danych osobowych[1] („RODO"), Szkoła jest administratorem Pani/Pana danych osobowych; pozyskiwanych w związku ze specjalnymi środkami wprowadzonymi z uwagi na istniejący stan epidemii COVID-19 na okres jego trwania, w celu ochrony życia i zdrowia pracowników i uczniów Szkoły.
2. Administrator wyznaczył Inspektora Ochrony Danych, z którym może się Pani/Pan kontaktować za pośrednictwem poczty elektronicznej pod adresem: DPO@aswarsaw.org.
3. Zakres Pani/Pana danych przetwarzanych przez Szkołę obejmuje następujące kategorie:
   a) dane dotyczące wysokości temperatury ciała;
   b) dane dotyczące stanu zdrowia, w szczególności dane o wynikach badań przesiewowych i diagnostycznych prowadzonych na zlecenie Szkoły przez EpiXpert Sp. z o.o. z siedzibą w Warszawie („**Dostawca**"), w tym zbiorczych testów antygenowych dla SARS-CoV-2, zbiorczych testów RT-LAMP dla SARS-CoV-2 i potwierdzających testów PCR;

GDPR Information Clause for Employees in connection with special measures during the COVID -19 epidemic

The American School of Warsaw with its registered seat in Bielawa, Warszawska 202, 05-520 Konstancin-Jeziorna (hereinafter referred to as the "**Controller**" or the "**School**"), using the website www.aswarsaw.org, informs that:

1. Pursuant to the provisions of the general data protection regulation[2] ("GDPR"), the School is the controller of your personal data collected in connection with special measures implemented due to the existing state of the epidemic of COVID-19 for the duration thereof, for the purposes of protection of life and health of the school employees and students.
2. The Controller has designated a Data Protection Officer, who can be contacted via e-mail at DPO@aswarsaw.org.
3. The scope of your data processed by the School covers the following categories:
   a) data related to body temperature;
   b) data related to the health condition, in particular data concerning results of screening and diagnostic tests performed at the request of the School by EpiXpert Sp. z o.o. with its registered seat in Warsaw (the "**Service Provider**"), including collective antibody SARS-CoV-2 tests, collective RT-LAMP SARS-CoV-2 tests, and PCR confirmation tests;

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

[2] 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).

c) dane o statusie nadanym Pani/Panu w aplikacji OK4School administrowanej przez Dostawcę („**Aplikacja**"), tj. zdolny/niezdolny do wejścia na teren Szkoły.

4. Pani/Pana dane osobowe, które Szkoła może przetwarzać, w celach określonych w pkt. 3 powyżej, obejmują dane dotyczące stanu zdrowia – w tym dane dotyczące wysokości temperatury ciała, a w razie zakażenia się przez Panią/Pana wirusem SARS-CoV-2 – również dane dotyczące zakażenia tym wirusem.

5. Dane określone w pkt. 3 lit. b) i c) powyżej zostały przekazane Szkole przez Dostawcę. Dostawca jako podmiot wykonujący działalność leczniczą jest odrębnym od Szkoły administratorem danych przetwarzanych w związku z testami i Aplikacją i przetwarza te dane w szczególności w celu udzielania świadczeń zdrowotnych, dokonywania rozliczeń z tego tytułu oraz prowadzenia, przechowywania i udostępniania dokumentacji medycznej. Szczegółowe informacje na temat zakresu danych przetwarzanych przez EpiXpert znajdują się w klauzuli informacyjnej EpiXpert dostarczonej Pani/Panu przed rozpoczęciem testów.

6. Pani/Pana dane osobowe mogą być przetwarzane w następujących celach:
   a) dane określone w pkt. 3 a) i b) powyżej (temperatura ciała, wyniki badań) będą przetwarzane w celu ochrony życia i zdrowia pracowników i uczniów Szkoły przed ryzykiem zakażenia wirusem SARS-CoV-2 przez zapewnienie im bezpiecznych i higienicznych warunków pracy (podstawa prawna: art. 9 ust. 2 lit. i) RODO w związku z art. 207 ustawy z dnia 26 czerwca 1974 r. - Kodeks pracy);
   b) dane określone w pkt. 3 c) powyżej (dane o statusie pracownika w Aplikacji) będą przetwarzane na podstawie Pani/Pana dobrowolnej zgody (podstawa prawna: 9 ust. 2 lit. a) RODO w związku z art. 22^{1a} § 1 Kodeksu pracy oraz art. 22^{1b} § 1 Kodeksu pracy). Zgodę na przetwarzanie danych może Pani/Pan w każdej chwili wycofać. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego

c) data on the status given to you in the OK4School application administered by the Service Provider (the "**Application**"), i.e. able/unable to enter the School premises.

4. Your personal data that the School may process for the purposes specified in point 3 above include health data – including data concerning the body temperature, and if you contract SARS-CoV-2 – also the data concerning the virus contraction.

5. The data specified in point 3 (b) and (c) above has been provided to the School by the Service Provider. The Service Provider as an entity operating medical activity is a controller separate from the School of the data processed in connection with the tests and the Application, and processes such data in particular in order to provide medical services, to bill such services and to keep, store and share medical documentation. Detailed information concerning the scope of data processed by EpiXpert is included in the EpiXpert information clause provided to you prior to testing.

6. Your personal data may be processed for the following purposes:
   a) data specified in point 3 (a) and (b) above (body temperature, test results) will be processed for the purposes of protection of life and health of school employees and students against the risk of contracting SARS-CoV-2 by assuring safe and hygienic work conditions (legal basis: Art. 9 (2)(i) GDPR in connection with Art. 207 of the Act of 26 June 1974 – the Labor Code);
   b) data specified in point 3 (c) above (employee's Application status) will be processed on the basis of your freely given consent (legal basis: Art. 9 (2) (a) GDPR in connection with Art. 22^{1a} § 1 of the Labor Code and Art. 22^{1b} § 1 of the Labor Code). You may withdraw your consent to data processing at any time. Consent withdrawal shall not affect the legitimacy of the processing carried out before the consent was withdrawn;

dokonano na podstawie zgody przed jej wycofaniem;

c) ponadto Pani/Pana dane określone w pkt. 3 powyżej, niebędące danymi szczególnych kategorii, o których mowa w art. 9 ust. 1 RODO, będą przetwarzane w celu realizacji prawnie uzasadnionego interesu Szkoły, polegającego w szczególności na dochodzeniu roszczeń przez Szkołę/obrony przed roszczeniami.

7. Pani/Pana dane osobowe mogą być przekazywane upoważnionym organom i instytucjom zgodnie z przepisami prawa, w szczególności organom sanitarnym na podstawie obowiązujących przepisów.

8. Pani/Pana dane osobowe będą także przekazywane dostawcom usług IT, dostawcom serwera w chmurze (np. Microsoft Azure) lub innym podmiotom, jeśli wymagają tego przepisy prawa.

9. Szkoła nie przekazuje ani nie zamierza przekazywać Pani/Pana danych osobowych do państw trzecich (poza Europejskim Obszarem Gospodarczym) lub organizacjom międzynarodowym.

10. Pani/Pana dane osobowe określone w pkt 3 powyżej będą przetwarzane wyłącznie dla celów, dla których zostały zebrane, przy czym:

    a) dane określone w pkt 3 stanowiące dane szczególnych kategorii będą przetwarzane przez okres 1 miesiąca od dnia ich pozyskania przez Szkołę. W przypadku, w którym dane te stanowią dowód w postępowaniu prowadzonym na podstawie prawa lub Szkoła powzięła wiadomość, iż mogą one stanowić dowód w postępowaniu, termin określony w zdaniu pierwszym ulega przedłużeniu do czasu prawomocnego zakończenia postępowania;

    b) dane określone w pkt 3, niestanowiące danych szczególnych kategorii, będą przetwarzane przez

c) moreover, your data specified in point 3 above, not being special category data referred to in Art. 9 sec. 1 GDPR shall be processed in order to pursue the legitimate interest of the School, consisting in particular in the School's exercise or defense of legal claims.

7. Your personal data may be shared with authorized bodies and institutions in accordance with the provisions of law, in particular, sanitary authorities on the basis of applicable regulations.

8. Your personal data shall be shared with IT service providers, cloud service providers (e.g. Microsoft Azure), or other entities, as required by legal regulations.

9. The School shall not share and does not intend to share your personal data with third countries (outside the European Economic Area) or international organizations.

10. Your personal data specified in point 3 above shall be processed solely for the purposes it has been collected for, whereby:

    a) data specified in point 3 being special category data shall be processed for the period of 1 month from the date it was collected by the School. If this data constitutes evidence in a proceeding conducted in accordance with the law or if the School learns that it may constitute evidence in such proceeding, the time limit specified in the first sentence shall be extended until the proceeding is finally concluded;

    b) data specified in point 3 not being special category data shall be processed for the limitation period of potential claims (6 years).

okres przedawnienia potencjalnych roszczeń (6 lat).

11. Na podstawie Pani/Pana danych osobowych Szkoła nie będzie podejmowała wobec Pani/Pana zautomatyzowanych decyzji, w tym decyzji będących wynikiem profilowania.

11. On the basis of your personal data, the School shall not take any automated decisions, including decisions resulting from profiling.

12. Posiada Pani/Pan prawo do żądania od Szkoły dostępu do danych osobowych dotyczących Pani/Pana, prawo ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz prawo do wniesienia sprzeciwu wobec przetwarzania danych, a także prawo do przenoszenia danych do innego administratora danych.

12. You have the right to demand that the School provides you with access to your personal data, the right of rectification or erasure of personal data, the right of restriction of processing, and the right to lodge a complaint against data processing, as well as the right of data portability.

13. Jeżeli sądzi Pani/Pan, iż przetwarzanie danych osobowych przez Szkołę narusza przepisy o ochronie danych osobowych, przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych. Biuro Urzędu Ochrony Danych Osobowych znajduje się w Warszawie (00-193) przy ul. Stawki 2, tel. 22 531 03 00, adres elektronicznej skrzynki podawczej: https://uodo.gov.pl.

13. If you believe that the School processes personal data in breach of the personal data protection regulations, you have the right to lodge a complaint to the President of the Personal Data Protection Office. The Personal Data Protection Office is located in Warsaw (00-193) at Stawki 2, tel. 22 531 03 00, electronic inbox address: https://uodo.gov.pl.

14. We wszelkich sprawach dotyczących Pani/Pana danych osobowych prosimy o kontakt z DPO@aswarsaw.org.

14. In any and all matters concerning your personal data, please contact DPO@aswarsaw.org.

W imieniu Administratora Danych / On behalf of the Data Controller: Jon P. Zurfluh

_____

Appendix 7 - GDPR Information Clause for Students and Parents in connection with special measures during COVID-19 epidemic

Konstancin-Jeziorna, **02/09/2020**

GDPR Information for Students and Parents in connection with measures during the COVID-19 epidemic

The American School of Warsaw with its registered seat in Bielawa, ul. Warszawska 202, 05-520 Konstancin-Jeziorna (hereinafter referred to as the "**Controller**" or the "**School**"), using the website www.aswarsaw.org, informs that:

1. Pursuant to the provisions of the GDPR [3], the School is the controller of parents' and students' personal data as previously authorized and collected in connection with special measures implemented due to the existing state of epidemic of COVID-19.
2. The School will process the following categories of data (hereinafter the "**Personal Data**"):
   a) students' body temperature;
   b) students' health-related data, in particular positive results of tests performed at the request of the School by EpiXpert Sp. z o.o. with its registered seat in Warsaw (the "**Service Provider**");
   c) students' status in the ok4School application of the Service Provider i.e. able/unable to enter the School premises;
3. The Personal Data specified in point 2 (b) and (c) above has been provided to the School by the Service Provider.
4. The Personal Data will be processed to protect life and health of the School's students and employees against the risk of contracting SARS-CoV-2.
5. The basis for processing Personal Data will be:
   a. the reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health (art. 9 sec. 2 i) GDPR);
   b. your consent (art. 9 sec. 2 a) GDPR). .
6. You may withdraw your consent to data processing at any time. Consent withdrawal shall not affect the legitimacy of the processing carried out before the consent was withdrawn. However, withdrawal of your consent may make it impossible to provide services under the terms of the enrolment contract.
7. Personal Data may be shared with authorized bodies and institutions, in particular sanitary authorities on the basis of applicable regulations, as well as IT service providers, cloud server providers (e.g. Microsoft Azure) or other entities, as required by legal regulations.
8. The School shall not share and does not intend to share Personal Data with third countries (outside the European Economic Area) or international organizations.
9. The School will retain Personal Data specified in point 2 (a) above for 1 day from the date it was collected by the School. The School will retain Personal Data specified in point 2 (b) and (c) above for the period of 1 month from the date it was collected by the School.
10. The School shall not take any automated decisions, including decisions resulting from profiling, on the basis of Personal Data.
11. You have the right to demand that the School provides you with access to Personal Data, the right of rectification or erasure of Personal Data, the right of restriction of processing and the right to lodge a complaint against data processing, as well as the right of data portability.

[3] 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

12. If you believe that the School processes Personal Data in breach of the personal data protection regulations, you have the right to lodge a complaint to the President of the Personal Data Protection Office.