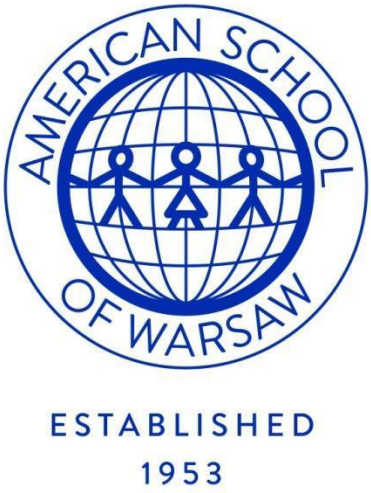

ASW Data Protection Policy & Procedures

Current Version Date	Next Projected Revision Date	Issuing date / Effective date
February 2021	June 2023	August 2022
Prepared by	**Checked by**	**Approved by**
DPO, Legal Review	Data Protection Committee, 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

1. 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.

2. 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

3. Definitions

- **ASW:** American School of Warsaw
- **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 subject:** a natural person whose personal data is processed by the controller or processor.
- **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.
- **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.
- **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.
- **processor:** a natural or legal person, public authority, agency or another body which processes personal data on behalf of the controller.
- **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)
- **School:** American School of Warsaw
- **Third country:** a country that is not a member of the European Economic Area.

4. Personal data processing principles

4.1. The Policy aims to provide the general framework for processing Personal Data by ASW.

4.2. The implementation of the Policy is aimed at ensuring compliance with the GDPR of processing of Personal Data by ASW, regardless of the form (electronic or paper) in which this processing takes place.

4.3. In connection with its activities, ASW collects and processes Personal Data in accordance with applicable law, in particular GDPR and the processing rules provided for therein, i.e .:

4.3.1. ASW ensures that the processing of Personal Data by him is lawful and is based on one of the bases of processing specified in the GDPR, i.e. in Article 6(1), Article 9(2) or Article 10 (principle of legality);

4.3.2. ASW ensures the reliability and transparency of personal data processing, in particular, it always informs about the processing of Personal data at the time it is collected, including the purpose and basis

legal processing (principle of fairness and transparency);

4.3.3. ASW ensures that Personal Data is collected in specific, clear and legitimate purposes and are not further processed in a manner inconsistent with these purposes (purpose limitation principle);

4.3.4. ASW ensures that Personal Data are processed only to the extent necessary to achieve the purpose for which the Personal Data was collected (principle of minimization);

4.3.5. ASW ensures that the Personal Data processed by him are correct and, when necessary, kept up to date, and that it is taking up all reasonable efforts to prevent Personal Data that is inaccurate in light of the purposes of their processing, have been immediately removed or rectified (principle of correctness);

4.3.6. ASW ensures that Personal Data is processed only for the period in which it is necessary to achieve the purposes of processing (time limit principle).

4.3.7. ASW ensures the security of Personal Data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, by implementing appropriate technical or organizational measures (principle of integrity and confidentiality).

4.3.8. ASW through appropriate technical and organizational measures, ensures the ability to demonstrate compliance of the processing of Personal Data with GDPR and other provisions on Personal Data (accountability).

4.3.9. ASW ensures constant compliance of the ASW's operations with the requirements of the protection of Personal Data provided for in the GDPR and other applicable legal provisions.

4.3.10. For this purpose, ASW, inter alia, monitors changes in legal provisions, guidelines of national and international data protection authorities personal data and the case law of courts and tribunals, and takes into account the best market practices.

4.3.11. ASW ensures compliance with the Policy by all ASW’s employees and associates.

4.3.12. ASW acknowledges that children merit specific protection with regard to their personal data as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.

5. Consent

5.1. The consent of the data subject is one (but not the only) basis for Personal data processing. Art. 6 GDPR (and art. 9 GDPR with respect to sensitive data) provides the conditions for the lawful processing of personal data and describes six lawful bases which ASW may rely on (including processing necessary for performance of a contract, processing necessary for compliance with a legal obligation, processing necessary for the purposes of the legitimate interests of ASW). The use of one of these six grounds, must be established prior to processing and with respect to a specific one target.

5.2. The consent shall be for example the basis for Personal data processing in following situations:

- use of students' photos in the school magazine / on the School website;
- processing of data in connection with participation in the film promoting the School
- processing of data by third parties, e.g. other schools implementing the project in which ASW students participate;
- disclosing the data of parents/students to a third-party company who intends to use it for direct marketing purposes.

The consent will not be the appropriate basis for the processing of personal data if the data is necessary for the performance of the contract with the data subject (e.g. for the performance of the Enrollment Agreement executed between the parent and the School) or where the basis for processing is legal obligation of ASW (ie. the school as an employer processes the data of employees).
Consent should rather not be used as the basis for the processing of personal data in connection with employment due to the dependence (imbalance) between the employee and the employer. It is unlikely that an employee will be able to freely respond to an employer's request for consent without feeling any pressure to consent.
In case of any doubts as to whether the consent should constitute the basis for data processing in a given case , please contact ASW Data Protection Officer. Every consent form should be drafted and/or reviewed by ASW Data Protection Officer.

5.3. If the basis for the processing of Personal data by ASW is consent of the data subject, ASW ensures that consent is:

- **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 ASW 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.

5.4. Where consent is given, a record will be kept documenting how and when consent was given. It is up to ASW to prove that valid consent was obtained from the data subject. The GDPR does not prescribe exactly how this must be done. However, ASW must be able to prove that a data subject in a given case has consented. As long as a data processing activity in question lasts, the obligation to demonstrate consent exists. After the processing activity ends, proof of consent should be kept no longer then strictly necessary for compliance with a legal obligation or for the establishment, exercise or defence of legal claims (Article 29 Working Party Guidelines on consent under Regulation 2016/679, page 20).

5.5. The consent of parents will be sought prior to the processing of a student's data who are under 18, except where the processing is related to preventive or counselling services offered directly to a student.

The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.

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.

It shall be as easy to withdraw as to give consent. In practice, if consent is granted electronically by one click of the mouse, by swiping or clicking a key, data subjects must be able to withdraw that consent in an equally easy way.

A statement of consent withdrawal will be forwarded in the electronic form to ASW at dpo@aswarsaw.org.

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.
Consent

6. Data subject rights

6.1. ASW exercises the rights of the data subjects on the basis specified in the GDPR, including:

6.1.1. the right to information about data processing - ASW provides the person submitting the request information on the processing of Personal Data, including in particular about the purposes and legal grounds of processing, scope of personal data held, entities, to which they are disclosed and the planned date of removal of Personal Data;

6.1.2. the right to access the data - ASW provides the data subject with a copy of the Personal Data concerning him/her;

6.1.3. the right to rectify data - ASW removes on request of the data subject possible inconsistencies or errors in the processed Personal Data and completes them if they are incomplete;

6.1.4. the right to erasure of the data - ASW removes or, upon request, anonymizes Personal Data, the processing of which is no longer necessary to pursue any of the purposes for which they were collected;

6.1.5. the right to restrict the data processing - ASW upon request ceases to perform operations on Personal Data - with the exception of operations for which the Data Subject has consented - and their storage, in accordance with the adopted retention rules or until the reasons for restricting the processing of Personal Data will not cease to exist;

6.1.6. the right to data portability - to the extent that Personal Data are processed in an automated manner, ASW issues the Personal Data data provided by the data subject in a format which allows for reading Personal Data by a computer;

6.1.7. the right to object to the processing of data for marketing purposes - the data subject may object at any time processing of Personal Data for marketing purposes, without necessity the reasons for such objection;

6.1.8. the right to object to other purposes of data processing - data subject can object at any time - for reasons related to his particular situation - to the processing of Personal Data, which takes place on the basis of a legitimate interest of ASW;

6.2. The detailed rules for exercising the rights of the data subjects by ASW are specified in the “Procedure for exercising the rights of persons whose personal data are processed by ASW” which constitutes Appendix [..] hereto.

7. Data Security

7.1. ASW as the data controller implements appropriate technical and organizational measures to ensure the level of security of Personal Data corresponding to the risk of infringement of rights or freedoms of natural persons with different likelihood of occurrence and weight threats. ASW takes into account the state of technical knowledge, the cost of implementation and the nature, scope, context and purposes of the processing.

7.2. When assessing whether the level of security is appropriate, ASW takes into account in particular the risk related to the processing, in particular resulting from accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to Personal Data transmitted, stored or otherwise processed.

7.3. To ensure the integrity and confidentiality of the Personal Data, ASW provides access to Personal Data only to authorized persons and only to the extent that it is necessary to perform their tasks. ASW uses organizational and technical solutions to ensure that all operations on Personal Data are recorded and implemented only by authorized persons.

7.4. ASW conducts an ongoing risk analysis related to processing Personal Data and monitors the adequacy of the security measures applied for identified threats. In case of emergency ASW implements additional measures to increase security Personal data.

7.5. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, ASW shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (DPIA).

7.6. 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.

7.6.1. 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.

7.6.2. 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.

7.7. 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.
- 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
- inform the DPO if any change occurs with respect to the personal data.

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

8. Responsibilities/Roles

8.1. 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.

8.2. Processing of Personal Data by ASW employees may only take place on the basis of documented authorization of ASW. In addition, ASW obliges authorized persons to maintain the confidentiality of Personal Data and information relating to security of Personal Data, as well as to comply with the Policy, including the procedures and rules regarding the protection of Personal Data in at ASW.

8.3. Data Protection Officer - ASW appoints a person responsible for the area of data protection, entrusting it with the function of Data Protection Officer and provides adequate resources to carry out the tasks entrusted to it.

Specific to Roles:

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/Contractors

- Any ASW employee/contractor has responsibilities in terms of collecting, using and storing personal data properly. Each ASW employee/contractor will read and sign the relevant informational clause.
- It is also the responsibility of each employee to process the Personal Data in accordance with this Policy, the authorization held and with due diligence.

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 internal policies and procedures of ASW;
- 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 isinformed 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.

9. Sharing and entrusting Personal Data

9.1. ASW shares the Personal Data with another controller only when one of the conditions referred to in Art. 6 sec. 1 GDPR or in art. 9 sec. 2 GDPR are fulfilled.

9.2. Entrusting the processing of Personal Data by ASW takes place based on a data processing agreement or other legal instrument referred to in art. 28 GDPR. ASW uses the template Data Processing Agreement.

9.3. Entrusting the processing of Personal Data by ASW takes place after prior verification that the processor provides sufficient guarantees of the implementation of appropriate technical and organizational measures, that the processing meets the requirements of the GDPR and protects the rights of the data subjects.

9.4. ASW also takes all necessary steps that also its subcontractors and other cooperating entities apply appropriate security measures in each case, when they process Personal Data at the request of ASW.

10. International Transfers

10.1. The level of protection of Personal Data outside the European Economic Area (EEA) differs from that provided by GDPR. For this reason, ASW transfers Personal Data to a Third country only when necessary and when the third country ensures the appropriate degree protection, primarily through:

10.1.1. cooperation with entities processing Personal Data in countries for which an adequacy decision have been issued by European Commission in which the Commission has decided that the third country ensures the adequate the level of protection of Personal Data;

10.1.2. use of standard contractual clauses issued by the European Commission.

11. Personal data breaches

11.1. ASW ensures reporting of personal data breaches to the supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

11.2. ASW ensures that he notifies data subjects without undue delay about teh breach of their personal data, if it can cause high risk of violation of their rights or freedom.

11.3. In any case, ASW examines the breach and implements the appropriate organizational and technical remedies.

11.4. ASW documents all personal data breaches, their effects and remedy.

11.5. The detailed procedure for dealing with personal data breaches constitutes Appendix [...] hereto.

12. CCTV and Photography

12.1. 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 7.

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.

12.2. Photography and Video Policy constitutes Appendix [...] hereto.

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

13. Final provisions

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

13.2. Appendixes 1-10 constitute an integral part of this Policy.

13.3. The School reviews yearly all the documents included in the Appendixes 1-10 in order to ensure that they comply with the GDPR.

13.4. The next scheduled review date for this policy is June 2023.

Appendix 1 - Personal Data Protection for 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 recipientsoutside the EU, 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 Personal Data Protection summary shall apply along with the ASW Data Protection Policy.

Appendix 2 - Personal Data Protection for Employees

Konstancin-Jeziorna, **01/04/2022**

Klauzula informacyjna dla pracowników / Information Clause for Employees

Pracownik/Employee: Xxxx Xxxx

W związku z zawarciem przez Panią/Pana umowy o pracę (dalej „**Umowa**") z:

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

1. Zgodnie z przepisami ogólnego rozporządzenia o ochronie danych osobowych[1] („**RODO**"), Szkoła jest administratorem Pani/Pana danych osobowych. Oznacza to, że odpowiadamy za wykorzystywanie Pani/Pana danych w sposób bezpieczny oraz zgodny z obowiązującymi przepisami prawa.

2. Pani/Pana dane osobowe przetwarzane są przez Szkołę w celu obsługi zatrudnienia oraz w celu realizacji obowiązków pracodawcy wynikających z przepisów szczególnych (w tym związanych z obowiązkowymi świadczeniami społecznymi i zdrowotnymi oraz w stosunku do organów podatkowych) (podstawa prawna: art. 22^1 Kodeksu pracy w zw. z art. 6 ust. 1 lit. c) RODO). Szkoła przetwarza także informacje dotyczące karalności w celu weryfikacji możliwości zaangażowania Pani/Pana do pracy z uczniami Szkoły oraz zapewnienia ich bezpieczeństwa (podstawa prawna: art. 10 RODO w zw. z art. 10 ust. 8a w zw. z art. 91b ust. 2b Karty Nauczyciela). Szkoła może też przetwarzać inne dane osobowe niż przewidziane w przepisach prawa (np. zdjęcie twarzy, informacje dotyczące karalności innych osób niż nauczyciele i wychowawcy, dodatkowe informacje dotyczące zdrowia) w celu obsługi zatrudnienia, weryfikacji możliwości zaangażowania Pani/Pana do pracy z uczniami Szkoły lub gdy jest to niezbędne do celów wynikających z prawnie

Since you are bound by a contract of employment (hereinafter the "**Contract**") concluded with:

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

1. Pursuant to the provisions of the General Personal Data Protection Regulation ("**GDPR**"), the School is the controller of your personal data. This means that we are responsible for safe and lawful use of your data.

2. Your personal data are processed by the School 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, as well as towards tax authorities) (legal basis: Art. 22^1 of the Polish Labour Code in connection with Art. 6(1)(c) GDPR). The School processes also criminal record information to verify, whether you are eligible to work with the students of the School and to assure the students' safety (legal basis: Art. 10 GDPR in connection with Art. 10(8a) in connection with Art. 91b (2b) of the Teacher's Charter). The School may also process personal data other than those stipulated in the provisions of law (e.g. facial image, criminal record information of persons other than teachers and educators, additional health-related information) for human resources purposes, verification of the possibility to engage you in work with the School's

[1] Rozporządzenia 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).

uzasadnionych interesów Szkoły, w tym zapewnienia bezpieczeństwa uczniów (art. 6 ust. 1 lit. f) RODO). Udzieloną zgodę można w każdym czasie wycofać.

students and for the purpose of assuring safety at the place of work based on consent granted by you (Art. 6 (1)(a) or Art. 9(2)(a) GDPR) or if it is necessary for the purposes resulting from the School's legitimate interests, including assuring the students' safety (Art. 6(1)(f) GDPR). The consent granted may be revoked at any time.

3. Podanie danych osobowych w zakresie zgodnym z art. 22^1 Kodeksu pracy lub przepisach szczególnych, jest wymogiem ustawowym. Brak podania tych danych spowoduje, iż Szkoła nie będzie mogła zawrzeć z Panią/Panem Umowy lub jej wykonywać, a także sprostać obowiązkom pracodawcy wynikającym z przepisów szczególnych. W zakresie danych, które możemy przetwarzać na podstawie Pani/Pana zgody, brak podania danych nie spowoduje jakichkolwiek negatywnych konsekwencji, jednak w pewnych sytuacjach może mieć to wpływ na ocenę Pani/Pana kwalifikacji z punktu widzenia obowiązków Szkoły w zakresie zapewnienia bezpieczeństwa uczniom oraz innym osobom przebywającym na jej terenie.

3. It is a statutory requirement to provide personal data in the scope specified in Art. 22^1 of the Polish Labour Code or in the specific provisions. Failure to provide such data will make it impossible for the School to conclude or perform the Contract with you, or to perform the employer's obligations resulting from specific provisions. With respect to data that we can process based on your consent, not providing us with them 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 safety of its students and other persons on its premises.

4. Ponadto Szkoła może przetwarzać Pani/Pana dane osobowe, w tym wizerunek, w celu zapewnienia bezpieczeństwa pracowników i uczniów Szkoły oraz w celu ochrony mienia, poprzez stosowanie monitoringu wizyjnego (podstawa prawna: art. 22^2 § 1 Kodeksu pracy w zw. z art. 6 ust. 1 lit. f) RODO). Szkoła może też przetwarzać Pani/Pana dane osobowe w celu zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz w celu właściwego użytkowania udostępnionych pracownikowi narzędzi pracy przy wykorzystaniu monitoringu Pani/Pana poczty elektronicznej oraz danych pobieranych przez udostępnione Pani/Panu narzędzia pracy w postaci służbowego telefonu komórkowego, tabletu, komputera itp. (podstawa prawna: art. 22^3 § 1 i 4 Kodeksu pracy).

4. Moreover, the School may process your personal data, including your image, to assure safety of the School's employees and students, as well as to protect property, through use of CCTV (legal basis: Art. 22^2 § 1 of the Labour Code in connection with Art. 6(1)(f) GDPR). The School may process your personal data in order to assure 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 computer, etc. (legal basis: Art. 22^3 § 1 and 4 of the Polish Labour Code).

5. Pani/Pana dane osobowe, które Szkoła może przetwarzać, obejmują imię i nazwisko, płeć, datę i miejsce urodzenia, obywatelstwo, dane kontaktowe (w tym numer telefonu i adres e-mail), adres zamieszkania, numer PESEL, numer zagranicznego ubezpieczenia społecznego, stan cywilny, numer dowodu osobistego lub paszportu, inne dane osobowe wynikające ze skanu dowodu osobistego lub paszportu, akt małżeństwa, akt urodzenia, numer prawa jazdy, charakter pobytu w Polsce, informacje dotyczące wykształcenia i kwalifikacji, w tym zdobytych uprawnień, informacje na temat doświadczenia zawodowego,

5. Your personal data that the School may process include: name and surname, gender, date and place of birth, nationality, contact details (including telephone number and e-mail address), address of residence, PESEL number, Social Security Number, marital status, ID card, passport, other data resulting from a scan of an ID card or passport, marriage certificate, birth certificate, driving licence number, nature of your stay in Poland, information concerning education and qualifications, including obtained licenses, information concerning professional

stanowisko, a także dane dotyczące wynagrodzenia, numer rachunku bankowego, dane dotyczące przebiegu zatrudnienia i oceny pracy, dane dotyczące członków rodziny pracownika korzystających ze świadczeń socjalnych, zakładowych lub z pomocy związanej z zamieszkaniem i pracą w Polsce, dane dotyczące nieobecności w pracy i związane z usprawiedliwianiem nieobecności w pracy, dane dotyczące stanu zdrowia –
w zakresie dopuszczalnym przepisami prawa oraz na podstawie udzielonej zgody (w przypadku wypełnienia formularza przez pracowników zagranicznych), zdjęcie twarzy do identyfikatora lub upoważnienia imiennego, informacje o niekaralności.

experience, function, as well as data concerning your remuneration, bank account number, data concerning the course of employment and work assessment, data of the employee's family members using social or company benefits or assistance in the scope of staying and working in Poland, data concerning absences from work and justifications of absences from work, health-related data – in the scope admissible under the provisions of law or based on consent granted (in case of filing in of the form by overseas hires), facial image for an ID or named authorisation, criminal record information.

6. Dane osobowe mogą być przekazywane uprawnionym organom oraz instytucjom na podstawie przepisów prawa.

6. Personal data may be shared with authorised bodies and institutions based on the provisions of law.

7. Dane osobowe obejmujące służbowe dane kontaktowe oraz dane zawarte w identyfikatorze służbowym lub nadanym upoważnieniu (w tym zdjęcie twarzy) mogą być przekazywane instytucjom współpracującym ze Szkołą oraz rodzicom uczniów. W określonych przypadkach udostępnieniu mogą podlegać dane potwierdzające uprawnienia zawodowe lub odbyte szkolenie BHP i przeciwpożarowe.

7. Personal data constituting business contact details as well as data on the business ID or in the authorisation granted (including facial image) may be shared with institutions cooperating with the School and with the parents of students. In specific cases we may also share data confirming professional licences or occupational safety and hygiene and fire protection trainings that the employee participated in.

8. Dane osobowe mogą być także przekazywane podmiotom przetwarzającym dane w imieniu Szkoły, uczestniczącym w wykonywaniu czynności przetwarzania danych przez Szkołę, tj.: podmiotom obsługującym systemy informatyczne i udostępniającym Szkole inne narzędzia informatyczne; podmiotom wydającym wizy/ pozwolenia na pobyt; podmiotom świadczącym Szkole usługi doradcze, konsultacyjne, rekrutacyjne, szkoleniowe, audytowe, podatkowe, rachunkowe. Pani/Pana dane Szkoła może przekazywać także innym administratorom przetwarzającym dane we własnym imieniu, tj. podmiotom prowadzącym działalność pocztową i kurierską; bankom lub instytucjom płatniczym.

8. 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, i.e.: entities operating the School's computer systems and providing it with IT tools; entities providing visa/ residence permit; entities providing for the benefit of the School, advisory, consulting, recruitment, training, audit, tax, accounting services. The School may share your personal data also to other data controllers processing data on their own behalf, i.e. entities providing courier or post services, banks and payment institutions.

9. Szkoła może przekazywać Pani/Pana dane osobowe do Stanów Zjednoczonych, Kanady, Nowej Zelandii i Australii w celach akredytacyjnych Szkoły oraz zapewnienia ubezpieczenia dla pracowników. W takim przypadku Szkoła podejmie działania wymagane do zapewnienia bezpiecznego przetwarzania danych przez podmioty z tych krajów zgodnie z przepisami prawa. Poza tym Szkoła przetwarza Pani/Pana dane osobowe z wykorzystaniem produktów i usług firmy Google, co może oznaczać przekazywanie danych do Stanów

9. The School may transfer your personal data to the United States, Canada, New Zealand and Australia for the School's accreditation purposes as well as to assure insurance for the employees. In such case 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. Additionally, the School processes your data with the use of Google products and services, which might mean that your data is transferred to the

Zjednoczonych. Bezpieczeństwo danych jest w tym przypadku zapewnione przez udział firmy Google w Programie Tarcza Prywatności UE-USA.

10. Pani/Pana dane osobowe będą przetwarzane przez czas trwania Umowy oraz w zakresie wymaganym przez przepisy prawa (dane zawarte w aktach osobowych i listach płac: osoby zatrudnione do 31 grudnia 2018 r. – przez okres 50 lat od zakończenia stosunku pracy; osoby zatrudnione od 1 stycznia 2019 r. – przez okres 10 lat od zakończenia stosunku pracy; pozostałe dane osobowe -przez okres 6 lat od końca roku, w którym ustał stosunek pracy). Nagrania z monitoringu wizyjnego będą przetwarzane przez okres 1 miesiąca od dnia nagrania. Jeżeli jednak będą prowadzone dochodzenia w sprawie popełnienia przestępstwa, okres przechowywania niezbędnych nagrań może zostać wydłużony.

11. Na podstawie Pani/Pana danych osobowych Szkoła nie będzie podejmowała wobec Pani/Pana zautomatyzowanych decyzji, w tym decyzji będących wynikiem profilowania. Profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

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.

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, e-mail: *kancelaria@giodo.gov.pl.*

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

United States. Safety of data in this case is guaranteed by Google's participation in the EU-USA Privacy Shield.

10. Your personal data will be processed during the term under the Contract as well as in the scope required under the provisions of law (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 from 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 will be processed for the period of 1 month from the date of recording thereof. However, if law enforcement is investigating a crime, images may be retained for a longer period.

11. 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.

12. You have the right to request that the School gives you access to your personal data, the right to have them corrected, deleted or their processing limited, the right to object against data processing, as well as the right to data portability.

13. 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), Stawki 2, 22 531 03 00, e-mail: *kancelaria@giodo.gov.pl.*

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

Pracownik: Potwierdzam, iż otrzymałem od Szkoły i zapoznałem się z zamieszczoną powyżej informacją o przetwarzaniu dotyczących mnie danych osobowych przez Szkołę, a także wyrażam zgodę na przetwarzanie moich danych osobowych w ww. zakresie
(gdy podstawą prawną jest moja zgoda).

Employee: I confirm that I have received from the School and I have read the above information concerning processing of my personal data by the School and, moreover, I agree to the processing of my personal data in the aforementioned scope (when my consent is the legal basis).

Pracownik (podpis) / Employee (signature):

Appendix 3 - 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 4 - Procedure for exercising the rights of persons whose personal data are processed by ASW

This document ("**Procedure"**) describes the procedures applied by the American School of Warsaw with its registered seat in Bielawa ("**ASW**" or "**Controller"**) to assure execution of the rights of data subjects whose data are processed by ASW as ASW within the EU General Data Protection Regulation) ("**GDPR**").

These procedures applies each time the data subject requests to exercise their rights ("**Requests**"), in particular:

1) **right of access to data**;
2) **right of rectification or completion of data**;
3) **right to erasure** ('right to be forgotten');
4) **right to restriction of processing**;
5) **right to data portability**;
6) **right to object against the processing of data** ;
7) **rights related to automated decision-making, including profiling**.

GENERAL RULES OF EXECUTION OF REQUESTS OF DATA SUBJECTS

1. The person responsible for dealing with the Requests at ASW is the ASW Data Protection Officer ("**DPO**").
2. Each time a DPO receives a Request, the DPO should verify whether ASW processes the personal data of the person submitting the request and whether the Request was submitted by an authorized person.
3. If DPO has reasonable doubts as to the identity of the person submitting the Request, she/he should request from such person additional information necessary to confirm her/his identity.
4. In a situation where the person cannot be identified on the basis of his/her data provided in Request, the DPO contacts this person in order to verify his identity. Verification takes place by requesting additional data from that person.
5. The deadline for replying to a Request is one month and may be extended by another two, but after informing the data subject in advance, together with the reason for the delay.
6. Responses to the Request should be made in the form in which the inquiry was received. If the data subject has transmitted his or her Request electronically, the information shall, as far as possible, also be transmitted electronically, unless the data subject requests another form, such as written form. Information may only be given orally if the data subject so requests and only if his or her identity is confirmed by other means.
7. The responses to the Requests should be made **free of charge**. By way of **exception**, the ASW may charge a **reasonable fee**, if the Request is unfounded or excessive, in particular because of their repetitive character (e.g. repetition of the same request at short intervals).
8. Each Request is entered in the register of data subjects' requests by the DPO ("Register"). The Register includes the data of the person submitting the Request, the subject of the Request, and the date of receipt of the Request.

1. RIGHT OF ACCESS TO DATA

Legal basis: Art. 15 GDPR

What may a data subject request?

- **confirmation**, whether ASW processes data of this person;
- **access** to personal data;
- obtaining the **information** listed in Article 15 sec. 1 GDPR
- receiving a **copy** of all personal data undergoing processing by ASW.

What is ASW obliged to do?

- verify if ASW processes the data subject's personal data and, if yes, **confirm** that to the data subject (e.g. via PowerSchool);
- provide the data subject with **access to the data** (e.g. by the electronic class register (PowerSchool), e.g. through a parent, student or employee account; providing access is not equivalent to the obligation to provide the data on a durable medium (paper or electronic) – this is subject to a specific right (cf. comments below).
- provide the **information** required by the data subject;
- provide the data subject with **a copy of any and all personal data** undergoing processing by ASW (the GDPR does not specify here the form of such a copy, it may be e.g. a PDF or another file containing a copy of the data). No scans or photocopies of documents shall be issued, as they may contain personal data not pertaining to the data subject submitting the request. The first copy shall be free of charge. For any further copies requested by the data subject, the ASW may charge a reasonable fee based on administrative costs (e.g. the actual cost of preparing and producing such a copy).

2. RIGHT OF RECTIFICATION OR COMPLETION OF DATA

Legal basis: Art. 16 GDPR

What may a data subject request?

- **rectification** of inaccurate personal data without undue delay;
- to have incomplete personal data **completed** (account taken of the purposes of processing), e.g. by means of providing a supplementary statement.

What is ASW obliged to do?

- rectify inaccurate data;
- complete personal data if they are incomplete;
- ASW is not obliged to complete the data with all the missing personal data (even if the data subject requests completion in this respect), but only with those data which correspond to the purposes of the processing;
- inform of the rectification each recipient to whom the personal data have been disclosed, unless this proves impossible or involves a disproportionate effort (Article 19 GDPR).

3. RIGHT TO ERASURE

Legal basis: Art. 17 GDPR

What may a data subject request?

- immediate erasure of data

What is ASW obliged to do?

- erase data if one of the following circumstances applies:
  - the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed (e.g. the legal period for processing the student's file has expired and there is no other basis for processing the data);
  - the data subject withdrew its consent (when processing is consent-based) and where there is no other legal ground for the processing, e.g. a specific statutory provision requiring data to be stored for a specific period);
  - the data subject lodged an objection to the processing of data and no overriding legitimate grounds for the processing (the right to object relates to processing based on the conditions specified in Art. 6(1)(e) and Art. 6(1)(f) GDPR);
  - the personal data have been unlawfully processed;
  - the personal data have to be erased for compliance with a legal obligation to which the ASW is subject;
  - the personal data have been collected in relation to the offer of a service provided by electronic means based on a child's consent.
- when ASW has made the personal data public and then the erasure has taken place, ASW should take reasonable steps to inform controllers which process the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data. ASW is not required to inform other controllers if it would be technically extremely difficult or impossible to do so.
- where erasure has taken place, ASW is obliged to inform of the erasure each recipient to whom the personal data have been disclosed, unless this proves impossible or involves a disproportionate effort (Article 19 GDPR). This is a separate obligation from the one mentioned above – it refers to data recipients, not controllers who process data as a result of their prior publication by the "original" controller.

ASW shall not be obliged to erase data to the extent that processing is necessary:

- for compliance with a legal obligation by ASW;
- for reasons of public interest in the area of public health (e.g. to assess the employee's ability to work);
- for the establishment, exercise or defense of legal claims (e.g. in the case of personal data contained in contracts, where the legal period for keeping such documents has expired, but the contract may be necessary in order to assert or defend against claims).

There are also other exclusions - please check art. 17 sec. 3 GDPR but they are unlikely to apply to ASW (freedom of expression, processing for reasons of public interest).

4. RIGHT TO RESTRICTION OF PROCESSING

Legal basis: Art. 18 GDPR

What may a data subject request?

- restriction of processing of personal data, i.e. cessation of data processing except for storage. ASW may continue to store the data, but any other processing operation shall be inadmissible

What is ASW obliged to do?

- restrict personal data processing, i.e. to cease personal data processing with the exception of storage, where:
  - the accuracy of the personal data is contested by the data subject – restriction for a period enabling ASW to verify their accuracy;
  - the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
  - the personal data are no longer needed for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims;
  - the data subject has objected to processing (cf. right to object) – restriction until such time as it is ascertained whether the legitimate grounds of ASW override the grounds of the data subject's objection;
- Where processing has been restricted – ASW may continue to store data, but any other processing operations are admissible only:
  - upon consent of the data subject;
  - for the establishment, exercise or defense of legal claims;
  - in order to protect the rights of another natural or legal person;
  - for overriding reasons of public interest of the Union or of a Member State.
- The request shall be recorded in the ASW's IT systems ensuring that the data are only stored and not used for any other purpose. This may be done e.g. by moving the data to a separate subset (system), temporarily blocking the data on a website (e.g. blocking a user profile) or otherwise blocking access to the data.
- Where processing has been restricted – the obligation to inform any recipient to whom the personal data have been disclosed of the data restriction, unless this proves impossible or involves a disproportionate effort (Article 19 GDPR);
- If processing restriction is lifted – the obligation to inform the data subject who requested the restriction.

5. RIGHT TO DATA PORTABILITY

Legal basis: Art. 20 GDPR

What may a data subject request?

- being provided in a structured, commonly used and machine-readable format with personal data that the data subject provided to ASW;
- for ASW not to hinder transmission of the abovementioned received data to another controller by the data subject;
- transmission of personal data by ASW directly to another controller (in the format indicated above), where technically possible.

In an educational unit, this right will be exercised very rarely.

What is ASW obliged to do?

- provide the data subject with all data that the data subject has supplied to ASW in a structured, commonly used and machine-readable format (e.g. XML, JSON, CSV).
- transmit the indicated data – upon request of the data subject – directly to another controller, if technically feasible.

What ASW can not do?

- hamper the data subject's right to transmit the data thus obtained to another controller, e.g. by requesting a fee for transmitting the data, failing to ensure an adequate format, intentionally masking out the filing system.

6. RIGHT TO OBJECT

Legal basis: Art. 21 GDPR

What may a data subject do?

- object to processing of his/her data personal data where:
    - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in ASW; or
    - processing is necessary for the purposes of the legitimate interests pursued by ASW or by a third party (e.g. for direct marketing purposes);
    - data are processed for scientific or historical research purposes or statistical purposes unless the processing is necessary for the performance of a task carried out for reasons of public interest.

When the objection is made, ASW should:

- no longer process the personal data unless ASW demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims;
- definitely stop processing - where personal data are processed for direct marketing purposes.

7. RIGHTS RELATED TO AUTOMATED DECISION - MAKING, INCLUDING PROFILING (ART. 22 GDPR)

ASW does not make any automated decisions or profiling referred to in Article 22(1) and (4) GDPR so this procedure does not describe the rights of the data subjects related to automated decision-making, including profiling (art. 22 GDPR).

Appendix 5 - Personal Data Breach Procedure

Purpose of the procedure

This procedure defines the steps that should be taken in the event of personal data breaches for which the American School of Warsaw ("ASW") is ASW.

What is a personal data breach?

1. General Data Protection Regulation ("GDPR") defines "personal data breach" as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (art. 4 point 12 GDPR).
2. Personal data breaches may for example include:
    - disclosure of personal data to an unauthorised person (e.g. a third party accidentally logging on to a student's account in the electronic class register (e.g. PowerSchool), an unauthorised person obtaining access to data as a result of infection of the ASW information system with malware);
    - temporary or permanent loss or destruction of personal data (e.g. loss or theft of media or device containing parent, student or employee data, accidental or unintentional deletion of data from the electronic class register (e.g.PowerSchool) by an employee);
    - unauthorised alteration of the content of personal data (e.g. unauthorised change of student details in the school system (e.g. PowerSchool).

Steps to follow in case of suspected personal data breach:

Step 1: Obtaining information on a personal data breach

If you suspect that a personal data breach has occured you should report it immediately to your supervisor and directly to the ASW Data Protection Officer at: dpo@aswarsaw.org, phone 22 7028500. In your report, please provide as many details about the breach as possible, in particular, date, time, place and description of the incident. Time to report identified data breach to authoritis is limited (72h), so all incidents should be investigated without delay.

Step 2: Assessing whether the incident constitutes a personal data breach

1. The ASW Data Protection Officer ("DPO") shall evaluate the incident and determine whether it is a personal data breach.
2. If the DPO decides that the incident is not a personal data breach, they shall inform the ASW Director (controller) of their findings. If the ASW Director upholds the decision of the DPO, the notification is considered cancelled and no further action is required.
3. If the DPO or the ASW Director decides that the reported incident is a personal data breach, it is necessary to proceed to the step described in § 5 below.

Step 3: Assessing whether the personal data breach needs to be reported to the DPA

The statement that there has been a personal data breach (security incident resulting in destruction, loss, unauthorized modification, disclosure or access to data) does not mean the need to report the breach to the data protection authority which in Poland is the President of the Personal Data Protection Office ("PUODO"). Art. 33 par. 1 GDPR obligates ASW to assess the probability that a personal data breach results in a risk of violation of the rights or freedoms of natural persons and:

a) if personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons, ASW may refrain from reporting the breach to PUODO.

b) if personal data breach is likely to result in a risk to the rights and freedoms of natural persons, ASW should report the breach to the PUODO,

Examples of situations when most probably the personal data breach needs to be reported (nonetheless, each such incident must be considered individually) include:

a) when a breach is likely to result (even potentially) in, e.g.:

- discrimination;
- identity theft or identity fraud;
- financial fraud (eg. if for example, third parties can use the data to obtain credit from non-bank institutions);
- financial loss;
- unauthorised reversal of pseudonymisation;
- loss of confidentiality of personal data protected by professional secrecy;
- damage to reputation or other significant economic or social disadvantage for the natural person affected.

b) if the breach involves "sensitive" personal data (eg. data revealing ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or genetic data, health or sex life data)

c) in situations, where documentation containing personal ID (PESEL) numbers has been lost or given to an unauthorised person.

If it is determined that a breach is likely to result in a risk to the rights or freedoms of natural persons, ASW shall notify PUODO of the breach in accordance with § 6 of the procedure.

Step 4: Notification to PUODO (if needed)

1. The minimum requirements for the content of the personal data breach notification are set out in Art. 33 GDPR.
2. Notification of the personal data breach should be made without undue delay and, where possible, not later than within 72 hours after having become aware of the breach.
3. Notification submitted to PUODO after 72 hours shall be accompanied by an explanation of the reasons for the delay.

4. Notifications can be made using the form available at www.uodo.gov.pl. Before sending the form, it is necessary to always refer to the current information on how to send the form, available at www.uodo.gov.pl.
5. It is possible to make a preliminary notification, if you don't know all the details about the breach at the time making the notification. In such case, please tick the 'Preliminary Notification' box on the notification form. You should provide the missing information as soon as you obtain them.

Step 5: Assessing whether communication to the data subjects is required

1. In each case, ASW should also assess whether it is required to notify the data subjects concerned about a data breach. The notification of data subjects is mandatory if the personal data breach is likely to result in a high risk to the rights or freedoms of natural persons.
2. The required content of the communication to the data subjects is set out in Art. 34 GDPR.
3. The notification of the data subjects should be made "without undue delay".
4. The notification shall be in a form that enables the data subject to repeatedly read the notification (e.g. e-mail, and in case of parents/students: a notification in the electronic class register - PowerSchool). Notifications should not be sent together with other information, for example newsletters or standard messages.

Documenting the personal data breach

1. In addition to the information obligations related to the personal data breaches (notifying the breach to PUODO and notifying the data subject about the breach), the GDPR requires ASW to document any personal data breach. Pursuant to Art. 33 paragraph 5 GDPR, ASW should document all personal data breaches, including the circumstances of the personal data breach, its effects and the remedial actions taken. In practice, this means the necessity to keep documentation of breaches, which should contain information about breaches found by ASW and about actions taken.
2. This documentation should allow PUODO to verify compliance with the requirements specified in GDPR in case of possible control.
3. The personal breach documentation may be kept in a form of a register, in an electronic or paper form.
4. The DPO is obliged to collect documents relating to the personal data breaches and if possible, indicate such documentation in the register for the purposes of possible future proceedings before PUODO.

Appendix 6 - Personal Data Retention Procedure

If you process personal data, please remember:

1. Personal data may not be processed indefinitely – they may be stored in a form that permits identification of the data subject for a period no longer than necessary for the purposes for which such personal data are processed (retention period).

2. To determine how long data can be stored, you should first determine whether the basis for the data processing is:

1) **contract** (=> you can process the data until the date of termination, expiry or performance of the contract, but please see point 3) or 4) as well);
2) **consent** (=> you can process the data until the consent is withdrawn by the person who gave it; consent is valid until its revocation);
3) **legitimate interest** of data controller (this is more complicated, see point 3. below);
4) **legal provision** (=>you can process the data until the end of retention period resulting from the provisions of law, please see the record of processing activities [link] for details).

3. Legitimate interests of the data controller may be the basis, for example, for:

- processing of customer data (e.g. parents) for marketing purposes;
- pursuing claims or defending against claims (see point 4 below);
- processing of the data to ensure IT security, including preventing unauthorized access to electronic communications networks and preventing damage to computer systems;
- ensuring authenticity and integrity of the media (IT systems) on which information, including personal data, is stored.

4. Processing for the purpose of pursuing claims may be carried out only until the claims are

time-barred, in particular:

a) civil law claims:

· claims under the Enrollment Agreement – 2 years,

· claims related to business activity or periodic benefits (e.g. resulting from a contract other than a service contract) – 3 years,

· other property claims – 6 years;

b) claims arising from employment relationships – 3 years;

c) claims relating to tax liabilities – 5 years.

5. You can see the detailed retention periods resulting from the provisions of law for individual Departments / areas in the record of processing activities of American School of Warsaw.

6. If different retention periods apply to the same data, the data should be stored for the longer retention period applicable.

7. If, before the end of the retention period, proceedings are initiated (e.g. a court case) that require data storage, the retention period is extended until the end of the proceedings.

8. After the end of the relevant retention period, the documentation should be destroyed or anonymized in a way that makes it impossible to identify the data subjects. For details, please contact our IT Department.

9. **Why is it important?**

A consequence of a GDPR violation in the scope of permissible personal data retention may be the administrative penalty (up to EUR 20,000,000, and in the case of a company – up to 4% of its total annual worldwide turnover from the previous financial year) or civil liability towards data subjects. There is also a risk of criminal liability for data processing without a legal basis!

10. In case of any questions, please contact the ASW Data Protection Officer:

e-mail: dpo@aswarsaw.org

phone: 48 22 702 8500

Appendix 7 - 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 8 - ASW Photography and Video Policy

The below Policy establishes the framework in which the American School of Warsaw("ASW") may take and use photographs or recordings of its students. It also describes the situations where parents and guardians are permitted to take photographs and record videos at designated school events.

Photographs and videos of ASW students may be taken by staff and students throughout the school year to record and share everyday life at ASW as well as, upon parents' consent, for marketing purposes and in external materials of ASW.

Legitimate interests

These images of ASW Students may be used based on legitimate interests of ASW for educational, safety and information purposes, including:

- in school ID Cards;
- for ASW's online administration system (PowerSchool);
- in internal ASW materials, e.g. eNotes, classroom projects, classroom blogs, and school displays

Consent

Using images or recordings of students for marketing purposes or in external publications, such as official website, school-managed social media, handbooks, school promotional publications either in digital or printed campaigns, requires the consent that parents grant at enrollment or re-enrollment.

While the school encourages all parents to provide consent, as this enables us to include all children in depictions of school life, we recognize and respect the right of parents to refuse consent. However, please note that a lack of the above consent may result in the student being asked to step away from the group when a photograph is taken so that their image is not included in the published materials.

Parents may withdraw consent at any time or grant consent if they had previously declined. Please note that in this situation, the processing of personal data carried out prior to such withdrawal will not be affected.

ASW may use photographs of students, without the prior consent of parents/legal guardians, in the school's legitimate interest, when photographs are necessary for identification purposes for making school ID cards and thus ensuring security on campus, or when such photographs are used for School's online administration system (PowerSchool).

The conditions of use of photos and videos

The photos and videos of the students may be used under the following conditions:

- Any material published online or in school publications should be assessed by the Communications Office to ensure it does not feature any child whose parent has not given consent.
- No photos and recordings must offer any means of identifying a child by name.
- When photographing children, the school will ensure all children are appropriately dressed.
- Images of large crowds wherein faces cannot be easily distinguished and therefore identified will not require the consent of each child photographed.
- The school will ensure that electronic images are stored on a secure network that cannot be accessed by members of the public.

Given the fact that photos and recordings are considered personal data, all the rights provided under the Privacy Notice dedicated to parents shall apply accordingly. In this respect, please consult the Privacy Notice available on the school's website at www.aswarsaw.org/privacynotice. ASW shall store the images and recordings of students for as long as they serve the purposes for which they were initially taken.

Use of camera phones and other recording devices by others

Visitors will be advised not to use their camera phones while at the school and where possible, will be accompanied by a staff member for the duration of their visit.

Rules for Parents and Guardians

Parents and guardians are permitted to take photographs and record videos at designated school events, as long as they agree to the conditions described in this policy. These events include:

- Musical Events
- Sport Tournaments
- Drama Productions
- Class Assemblies
- Graduation activities
- PTO Events i.e. Color Run, Fall, and Spring BBQ
- Maker Faire
- New Family Orientation Day
- Traditional holiday-related events i.e. Carnival
- UN Day
- Studniówka

At these events, photos may only be taken at the location of the event that depicts the event itself. For most of these, this is the school theatre, gyms, sports fields. Parents and Guardians are not permitted to take photos in classrooms or elsewhere in the school unless explicitly authorized by the school principal. Outside designated events, it is not permitted to use a camera on school premises at any time outside these designated events unless explicitly authorized by the school principal.

Distribution and publication of photos and videos

Where parents or students' families or students take photos or videos of other students on school premises or in the context of various school events or activities, for purely personal, household or recreational purposes, the school shall not bear any responsibility with regard to the use of those photos or videos. The above pertains to photos and videos taken at ASW events off-campus as well (such as the graduation ceremony).

The school hereby kindly requests parents to use all images and video taken as described above with maximum regard to the rights and liberties of other persons, especially children appearing in those photos or videos.

Where students or parents will take photos or videos for official use of the school, ASW shall take care that these photos will be handled and used according to this Policy.

Appendix 9 - 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:_____

Appendix 10 - 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[2] („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

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[3] ("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

[2] 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).

[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 (General Data Protection Regulation).

RT-LAMP dla SARS-CoV-2 i potwierdzających testów PCR;

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

RT-LAMP SARS-CoV-2 tests, and PCR confirmation tests;

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

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 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.

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;

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

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. 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.

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

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. 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

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

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 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.

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.

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.

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

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).

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

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

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 [4], 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.
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.

[4] 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