ASW Data Protection Policy

May, 2018

ASW Mission Statement

We believe there are many paths to learning. To unlock our students' potential, we provide a wide range of experiences: we engage them in our rigorous academic curriculum, visual and performing arts programs, athletics, and service learning. We foster a passion for ideas, creativity and curiosity.

We create a culture of learning that supports students with a diverse set of abilities and interests. We challenge students to find their own voices, encourage them to ask questions, and inspire them to think for themselves.

We offer students and their families a welcoming, inclusive and safe environment, one that is balanced between our host country Poland and the international community. We treat all students with respect, and we instill in them respect for others. Our students form friendships that remain lifelong connections.

Rationale

As indicated in Board Policy 5.03, the American School of Warsaw (ASW) is committed to the protection of all personal and sensitive data for which it holds responsibility of as the Data Controller.

This policy is in place to provide the school with the organizational procedures for handling such data in compliance with current data protection principles and the European General Data Protection Regulation (GDPR) 2016/679.

Table of contents

Objective and Legal Framework

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

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

- Complies with data protection law, including GDPR and 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.
- Adequate safeguards are implemented 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 student/parents.

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

Policy Framework

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

5.03 Personal Data Protection

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

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

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

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

Revised: June, 2018

Terminology

- **Personal data**: any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **Sensitive personal data:** any information relating to an identified or identifiable natural person revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data. Data relating to criminal offences and convictions are addressed separately (as criminal law lies outside the EU's legislative competence).
- **Data Processing:** any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **Restriction of processing:** the marking of stored personal data with the aim of limiting their processing in the future.
- **Data controller:** the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
- **Data processor:** a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- **Data recipient:** a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
- **Data Subject:** A natural person whose personal data is processed by a data controller or processor.
- **Third Party:** a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.
- **Consent:** any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- **Data breach:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

- **Representative**: a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation.
- **DPO**: Data Protection Officer
- **GDPR:** Regulation (EU) 2016/679 of the European Parliament and of the Council, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and follows good practice;

Any additional terms related to data protection shall have the meaning designated to them under article 4 of the GDPR.

Personal data processing principles

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

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

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

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

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

Personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

- **Processed in a manner that ensures appropriate security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. This includes both technical and organisational measures such as defined processes and training and awareness.
- **Lawfully transferred outside the European Economic Area**: ASW will only transfer personal data outside the European Economic Area where the relevant agreement with this supplier is in place to accommodate all the safeguards imposed by the data protection applicable legal provisions.
- **Lawfully transferred to third parties:** ASW shall transfer personal data to a third-party controller to the extent necessary to serve the applicable legitimate purposes for which the personal data are processed. Transfer to a third party must be in accordance with the respective legal and regulatory requirements.

  Data transfer is always allowed in the following situations:

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

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

Accountability

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

ASW will provide comprehensive, clear and transparent privacy policies.

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

- Name and details of the organisation.
- Purpose(s) of the processing.
- Description of the categories of individuals and personal data.
- Retention schedules.
- Categories of recipients of personal data.
- Description of technical and organisational security measures.
- Details of transfers to the third countries, including documentation of the transfer mechanism safeguards in place.
- Legal basis for processing.

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

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

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

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

ASW will ensure that all DPIAs include the following information:

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

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

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

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

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

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

Sensitive data processing

Sensitive data will only be processed under one of the following conditions:

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

Consent

Consent must be:

- **freely given** and should reflect the data subject's genuine and free choice without any element of compulsion, or undue pressure put upon the data subject, avoiding any negative consequences in the case of refusal to give it.
- **specific**: ASW must clearly and precisely explain the scope and the consequences of the data processing.
- **informed**: the nature of the processing should be explained in an intelligible and easily accessible form, using clear and plain language which does not contain unfair terms. The data

subject should be aware at least of the identity of the controller and the purposes for which the personal data will be processed.

- **explicit in a positive indication**: ASW will consider written declarations, email responses, and active checkboxes. Consent can not be inferred from silence, inactivity or pre-ticked boxes.

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

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

Direct marketing

ASW shall engage in unsolicited commercial communication (direct marketing communication) only with the prior consent of the Individual ("opt-in"). In every direct marketing communication that is made to the individual, the individual shall be offered the opportunity to opt-out of 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 data subject.

Objection to direct marketing

If an individual objects to receiving marketing communications, or withdraws his 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.
ASW accepts a written statement signed by the data subject which specifies the exercise of the right to object to direct marketing. It should be forwarded to ASW at dpo@aswarsaw.org

Additionally, ASW keeps records to demonstrate that a valid consent has been given and that the data subject has been informed.

Withdrawal of consent

Data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. ASW accepts a written statement signed by the data subject which specify the exercise of the right of withdrawal the consent. It will be forwarded in electronic form to ASW at dpo@aswarsaw.org

Data subject rights

Right to be informed

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

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

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

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

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

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

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

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

Right of access

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

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

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

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

Where a SAR has been made electronically, the information will be provided in a commonly used

electronic format, unless otherwise requested by the data subject.

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

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

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

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

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

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

Right to rectification

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

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

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

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

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

Right to erasure

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

Individuals have the right to erasure in the following circumstances:

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

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

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

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

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

Where personal data has been made public, ASW, taking account of available technology and the cost of implementation, will take reasonable steps to inform other controllers who process the personal data that the data subject has requested the erasure by such controllers of any links to and copies of the personal data in question.

Right to restrict processing

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

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

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

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

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

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

Right to data portability

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

services.

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

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

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

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

ASW will provide the information free of charge.

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

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

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

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

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

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

Right to object

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

Individuals have the right to object to the following:

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

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

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

Where personal data is processed for direct marketing purposes:

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

Where personal data is processed for research purposes:

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

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

General provisions regarding data subject rights requests

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

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

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

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

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

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

Data Security

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

Printed data:

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

Electronic data:

- Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.
- Where data is saved on removable storage or a portable device, the device will be kept in a

locked filing cabinet, drawer or safe when not in use.

- Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.
- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Best practices:

- Data will be held in few places as necessary. Staff should not create any unnecessary additional datasets.
- Where possible, ASW enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- Employees will not use their personal laptops, computers or mobile devices for ASW purposes.
- All employees are provided with their own secure login and password which will be regularly changed.
    - Employees must use strong passwords. Passwords must be kept confidential and changed regularly.
- Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.
- Before sharing data, all staff members will ensure:
    - They are allowed to share it.
    - That adequate security is in place to protect it.
    - Who will receive the data has been outlined in a privacy notice.
- Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of ASW containing sensitive information are supervised at all times.
- The physical security of ASW buildings and storage systems, and access to them, is reviewed on a termly basis If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.
- Personal data should not be disclosed to unauthorized people, either within ASW or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their department manager or the Data Protection Officer if they are unsure about any aspect of data protection.
- User should not circumvent computer security or gain access to a system for which they have no authorization.

- Servers and workstations will be protected by using security software and implementing firewall rules. They will also be located in places specially equipped with access control and environmental controls, inaccessible to unauthorized persons.
- Data must be frequently backed up and these copies must be periodically tested to ensure data recovery.
- The access to IT systems (to personal data) will be granted by the IT department under 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 to accomplish other objectives, such as preserving intellectual property and cost management.

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

Responsibilities

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

Any ASW employee has responsibilities in terms of collecting, using and storing personal data properly. At the same time, the departments and teams are responsible for developing their own operational **procedures** to ensure that in terms of personal data the good practices are established and respected.

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

Data protection officer

A DPO will be appointed in order to:

- Inform and advise ASW and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the schools 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.
- Report to the highest level of management at ASW, which is the School Director and Board of Trustees.
- Handle Subject Access Requests.
- Check and approve any contracts or agreements with third parties that may contain sensitive data.

The DPO will:

- have control and monitoring powers (the right to perform internal investigations and to access information).
- have expert knowledge of data protection law and practices.
- be able to operate independently without conflict of interests with its other professional duties.

Employees with access to personal data

- only access personal data to the extent necessary to serve the applicable legitimate purposes for which ASW processes personal data and to perform their job.
- report of any (possible) incident or issue relating to personal data to their manager or to the DPO.
- never discuss confidential information in public areas or with individuals who don't have a need to know.
- dispose of sensitive documents properly and log the disposal.
- computing devices should be powered off when not in use for extended periods of time (such as after work, on weekends, during holidays and so on).
- users working in departments that handle confidential information should lock and secure all information and equipment when they are away from their desk areas.
- users should keep their desk areas organized and keep all confidential information secured and out of view when away from their desks.
- not sharing of passwords.
- not storing the passwords in plain text.
- user should promptly report any suspected breach of security policy that comes to their knowledge.
- consult the DPO and/or the direct manager whenever they have concerns regarding the data privacy.

Director

- Ensure that an adequate organizational structure is in place as well as effective communication and reporting channels, in order to ensure that personal data is being processed in a clear and consistent way and in compliance with the ASW internal policies and procedures;
- Work 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);
- 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 Department will process personal data in accordance with this policy.
- Ensure that ASW staff is informed with regard to policies and procedures relevant to the protection of personal data.

- Ensure that personal data are processed in accordance with procedures and policies relevant to the protection of personal data.
- Notify the DPO and follow his advice on emerging risks or incidents.
- Ensure that the data inventory process is correct and complete. The data inventory of personal data must be updated periodically.
- Ensure that the staff working in his department follow the required training.

Director of ICT

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the company is considering using to store or process data in order to ensure the integrity, confidentiality and availability of processed data. For instance, cloud computing services.
- Identify and implement technical measures to ensure the security of personal data stored.
- Provide support for investigating potential breaches of security;
- Provide personnel training on technical and security standards for the processing and protection of personal data.

Director of Communications and Marketing

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

Director of Human Resources

- identifying the training and development needs of the staff in connection to 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 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. HR Manager must ensure a balance between the interests of ASW and the right to a private life of employees.

Publication of information

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

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

CCTV and Photography

ASW understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

ASW notifies all students, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

All CCTV footage will be kept for 3 weeks for security purposes; the Security Manager is responsible for keeping the records secure and allowing access.

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 student, school ID card, diploma/report cards and other official document)
- Yearbook.

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

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

Policy review

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

The next scheduled review date for this policy is May 2019.