Polish British Academy of Warsaw

Primary School

Data Protection Policy

PBAW Headmistress: Maria Fiedorczuk-Piechota

Governors: Magdalena Eysmont, Monika Konieczna-Kowalczyk

Approval date: 20th September 2022

Policy is: PUBLIC

Review date: July 2023

Purpose
This policy sets out how the school deals with personal information, in accordance with the Data Protection Act of 29 August 1997 and other related documents. This policy applies to all personal information however it is collected, used, recorded or stored and whether it is held on paper or electronically.

All school staff and governors involved in the collection, use, processing or disclosure of personal data will be aware of their duties and responsibilities and will adhere to this policy.

PBA uses and collects personal information (referred to in the Data Protection Act as personal data) about:

- staff
- pupils
- parents / guardians
- other individuals who come into contact with the school.

This information is gathered in order to enable the provision of education and other associated functions.

The school is obliged (by law) to collect, use and share certain information.

What is personal information / data?
In accordance with Art. 6 paragraph. 1 of the Act of 29 August 1997 on the protection of personal data (i.e. Dz. U. of 2002. No. 101, item. 926, as amended), personal data means any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social features (art. 6, paragraph. 2 of the Act). Personal data will, therefore, contain both data that are used to determine the identity of the individual, as well as those that do not allow for the immediate identification, but are (with some effort, time and activity) sufficient to its findings. Such data will be the personal information that allows the identification of a person, without extraordinary effort and investment, especially with the use of easily accessible and widely available sources.

In light of this definition, it must be assumed that personal data will not be individual information with a high degree of generality, e.g. personal address details or salary. This information will, however, be considered personal when it is paired with any additional information, which can consequently be applied to a particular person. An example of a single personal information that is given is, however, National Identity Number, which, according to Art. Paragraph 31a. 1 of the Act of 10 April 1974 - Population Census and Identity Cards (Dz. U. of 2001. No. 87, item. 960, as amended), is a 11-digit, numeric constant symbol that uniquely identifies an individual (the first six digits represent the date of birth - year, month, day, another four - the ordinal number and sex of the person, and the last is a check digit given for the accuracy of the registration number. It can be concluded that

the social security number by definition is given personal, and it is subject to all the rigours of processing provided for in the Act on the Protection of Personal Data.

The legislature formulating Art. 6 of the Act on the Protection of Personal Data, used a general clause, thus not specifying an exhaustive list of information constituting personal information. Therefore, when deciding whether specific information constitutes personal data, in most cases, it is inevitable to make an individual assessment, taking into account the specific circumstances and the type of media or methods necessary in a particular situation to identify the person.

Personal data includes (but is not limited to):

- an individual's, name, address, telephone number
- date of birth / birth certificate
- photographs
- financial information
- PESEL- Personal Identity Number
- ID card / passport
- details such as religion or health records
- family status details
- diplomas or certificates

What is sensitive personal data?

Sensitive personal data is identified separately because further conditions need to be applied before it can be used. Explicit consent from the person concerned is usually required before the details can be shared or passed to others in order to provide a particular service. Of course, there are times when our 'duty of care' or legal duty requires us to inform others, e.g. following an assessment of identified risks relating to a specific individual.

Sensitive personal data includes information as:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs, religious affiliation, party or trade union
- health, genetic code, addictions or sex life
- convictions, decisions about penalties and fines, as well as other decisions issued in judicial or administrative proceedings

The processing of this information is permitted only in the cases enumerated in the Act:

- the data subject has given their consent in writing
- another law allows the processing of such data without the consent of the data subject and provides adequate safeguarding
- processing is carried out in order to protect the health, the provision of medical services or treatment of patients
- processing relates to data that have been made public by the data subject

Data protection principles

- an employee has the right to access their personal data, which is held for employment purposes (this does not include information processed by them as part of their role at work)
- one should speak to the HR Coordinator if they wish to see their own personal records and if their circumstances change, e.g. they move home (they should ensure they notify the HR Coordinator of such changes, in order to maintain accuracy of the information that the school holds)

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specified and lawful purpose.
3. Personal data shall be adequate, relevant and not excessive.
4. Personal data shall be accurate and where necessary, kept up to date.
5. Personal data processed for any purpose shall not be kept for longer than necessary.
6. Personal data shall be processed in accordance with the rights of data subject under the Data Protection Act.
7. Personal data shall be kept secure, i.e. protected by an appropriate degree of security.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of data protection.

Commitment

The school is committed to maintaining the above principles at all times. Therefore, the school will:

- inform individuals why personal information is being collected
- inform individuals when their information is shared, why and with whom, unless the Data Protection Act provides a reason not to do this
- obtain consent before processing Sensitive Personal Data, even if consent is implied within a relevant privacy notice, unless one of the other conditions for processing is found in the Data Protection Act
- check the accuracy of the information it holds and review it at regular intervals
- ensure that only authorised personnel have access to the personal information whatever medium (paper or electronic) it is stored in
- ensure that clear and robust safeguarding practice is in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- ensure that personal information is not retained longer than it is needed
- ensure that when information is destroyed that it is done so appropriately and securely
- share personal information with others only when it is legally appropriate to do so
- comply with the duty to respond to requests for access to personal information, known as Subject Access Requests
- ensure that personal information is not transferred outside the EEA without the appropriate safeguarding practice
- ensure all staff and governors are aware of and understand these policies and procedures

Complaints
Complaints will be dealt with in accordance with the school complaints/allegations policy. Complaints relating to handling of personal information may be referred to the Information Commissioner.

Review
This policy will be reviewed as it is deemed appropriate, but no less frequently than every two years. The policy review will be undertaken by the Headmistress, or a nominated representative.

If you have any enquiries in relation to this policy, please contact the Headmistress, who will also act as the contact person for any Subject Access Requests.