

**Polish British Academy of Warsaw**

**Primary School**

**and**

**Kids' Academy Preschool**

**Data Protection Policy**

**Headteachers:**

Head of the Primary: Kamila Wilczyńska

Head of Preschool: Mirosława Bejgier

**Superiors name:** Magda Eysmont, Monika Konieczna-Kowalczyk

**Approval date:** 1st March 2015

**Policy is:** PUBLIC

## **PURPOSE**

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

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

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

- staff
- pupils
- parents
- others 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 required 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 (ie 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 a person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social (art. 6, paragraph. 2 of the Act). Personal data will therefore 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 they are, with some effort cost, time and activities sufficient to its findings. Such a 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. Beyond the scope of this definition will therefore such information, based on which identification will require unreasonable, disproportionate effort cost, time or activities.

In light of this definition, it must be assumed that personal data will not be individual information with a high degree of generality, eg. Name of the street and house number or salary. This information will, however, be given personal when it is paired with any additional information, which consequently can 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, in 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 is used to control a computer given to 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 rigors 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 specify an exhaustive list of information constituting personal information. Therefore, when deciding whether specific information or 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
- sensitive details such as religion, health records or ethnic origin
- family or 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 those 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, perhaps

For example, 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 his consent in writing,

- another law allows the processing of such data without the consent of the data subject, and provides adequate safeguards,
- 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, it is necessary to do research, provided data anonymous

## **DATA PROTECTION PRINCIPALS**

- An employee has the right to access your personal data, which is held for employment purposes. (This does not include information processed by you as part of your role at work)
- Speak to the Office Manager representative if you wish to see your own personal records and if your
- Circumstances change, e.g. you move home, please ensure you notify your Manager in order to maintain accuracy of the information that we hold about you

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 for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data subject under the Data Protection
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, and 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 in the Data Protection
- 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 safeguards are 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 safeguards
- 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's complaints policy. Complaints relating to the handling of personal information may be referred to the Information Commissioner who can be contacted

#### 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 Headteacher, or nominated representative.

#### CONTACTS

If you have any enquires in relation to this policy, please contact the Head Teacher who will also act as the contact point for any subject access requests.