Pushkin's School of Russian Language and Literature

GDPR and Data Protection Policy (2019-2020)

Date agreed: December 2019.

Date of next review: July 2020.

Approved by: Elena Vlasenko (School Director)

General Data Protection Regulation 2018 (GDPR) and the Data Protection Act 2018 (DPA) are the legislation that protect personal privacy and uphold an individual's rights. It applies to anyone who handles or has access to people's personal data. This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with current legislation. It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

Policy Objectives

Pushkin's School, the Data Controller, will comply with its obligations under the GDPR and DPA. The school is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure that data subjects (pupils, parents/carers, staff and volunteers) are aware of their rights under the legislation.

All staff must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All staff must read, understand and comply with this policy. The Information Commissioner as the Regulator can impose large fines for serious breaches of the GDPR, therefore it is imperative that all staff comply with the legislation.

Scope of the Policy

Personal data is any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the information (GDPR Article 4 Definitions). The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living individual. This includes any expression of opinion about an individual and intentions towards an individual. Under the GDPR, personal information also includes an identifier such as a name, identification number, location data or an online identifier.

Pushkin's School collects personal data every year on pupils, parents and staff, which includes, but is not limited to:

- Pupil's full name, date of birth, nationality, place of birth, home address, Pushkin's School branch and the public/private school that they attend. If applicable, SEN requirements, disabilities and medical information are also recorded.
- Parent's/carer's full name, home address, personal phone number, email address, job role and business phone number.
- Staff member's personal information, contact details, bank details, National Insurance, recruitment information, DBS certificate, copy of driving licence, medical conditions and sickness records.

The Principles

The principles set out in the GDPR must be adhered to when processing personal data:

1. Lawfulness, fairness and transparency – personal data shall be processed lawfully, fairly and in a transparent manner.
2. Purpose limitation - personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Data minimisation – personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed.
4. Accuracy – personal data shall be accurate and where necessary kept up to date and every reasonable step must be taken to ensure that inaccurate personal data is erased or rectified without delay.
5. Storage limitation – personal data shall be kept in a form which permits identification of data subjects for no longer than necessary for the purpose for which the personal data is processed.
6. Integrity and confidentiality – appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal information is processed in a manner that provides appropriate security to the personal data. This security shall protect against unauthorised or unlawful processing of personal data, as well as the accidental loss or destruction of, or damage to, personal data.
7. Transfer limitation – personal data shall not be transferred to a country outside the European Economic Area without adequate protection for the rights and freedoms of the data subjects.

Lawful Basis for Processing Personal Information

Prior to processing any personal information, the purpose for the processing activity and the most appropriate lawful basis must be selected. Processing is necessary for:

- the performance of a task carried out in the public interest or in the exercise of official authority vested in the school;
- the performance of a contract to which the data subject is a part of;
- compliance with a legal obligation to which the data controller is subject to;
- the protection of vital interests of the data subject or of another person;
- the legitimate interests pursued by the data controller or by a third party;
- one or more specific purposes for which the data subject has given consent to process. Consent can be withdrawn at any time and this will be promptly honoured. Consent may need to be reviewed if personal data is intended to be processed for a different or incompatible purpose which was not disclosed when the data subject first gave consent.

Sensitive Personal Information

Processing of sensitive personal information (known as 'special category' data) is prohibited unless a lawful special condition for processing is identified (GDPR, Article 9). Personal data is 'special category' if it relates to racial or ethnic origin, political beliefs, religious or philosophical beliefs, trade union membership, genetic or biometric data, physical or mental health, or sexual orientation.

Sensitive personal information will only be processed if there is a lawful basis for doing so or if one of the following special conditions apply:

- the data subject has given explicit consent;
- the processing is necessary for the purpose of exercising the employment law rights or obligations of the school or the data subject;
- the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;

- the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, associations or any other not-for-profit body with a political, philosophical, religious or trade-union aim;
- the processing relates to personal data which is manifestly made public by the data subject;
- the processing is necessary for the establishment, exercise or defence of legal claims;
- the processing is necessary for reasons of substantial public interest;
- the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services; or
- the processing is necessary for reasons of public interest in the area of public health.

All sensitive personal information processed by Pushkin's School, what it is used for, the lawful basis for the processing, and the special condition that applies is set out in the school's Staff Privacy Notice and Pupil and Parent Privacy Notice. Sensitive personal information will not be processed until an assessment has been made as to whether the processing complies with the criteria above, the purpose for which it is being carried out and the legal basis for it. Explicit written consent will be required and recorded when processing any type of sensitive personal data.

Documentation and Records

The Data Protection Officer (DPO) for all Pushkin's School branches is Anton Vlasenko (School Administrator). The DPO is responsible for keeping and recording all written records of processing activities. The DPO will record the following information:

- the name and details of individuals or roles that carry out the processing;
- the purposes of the processing;
- a description of the categories of individuals and the categories of personal data;
- categories of recipients of personal data;
- data Retention Schedules;
- a description of technical and organisational security measures;
- information required for Privacy Notices;
- records of written parental consent;
- contracts;
- the location of personal information; and
- records of data breaches.

Pushkin's School will conduct regular reviews of the personal information it processes and will update all documentation accordingly. This policy will be reviewed annually to address retention, security and data sharing.

Privacy Notice

The Pupil and Parent Privacy Notice informs the data subjects (or their parents if the data subject is under 16 years of age) about the personal information that the school collects and holds relating to individual data subjects. It also details how individuals can expect their personal information to be used and for what purposes. Pushkin's School Privacy Notices can be found on the school's website (www.pushkinsrussianschool.co.uk/policies).

Pushkin's School has two Privacy Notices, one for pupil and parent information and one for staff information. Appropriate measures have been taken to provide Privacy Notice information in a concise, transparent, intelligible and in an easily accessible form, using clear and plain language. The Privacy Notices will be reviewed in line with any statutory or contractual changes.

Purpose Limitation

Personal data will only be collected for specified, explicit and legitimate purposes. Personal data will not be used for new, different or incompatible purposes that were not disclosed when consent was first obtained. The only exception is when the data subject has been informed of the new purposes and has given written consent.

Data Minimisation

Personal data will be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. Staff may only process data when their role requires it. Staff must not process personal data for any reason that is unrelated to their role.

The DPO maintains a Retention Schedule to ensure that personal data is deleted after a reasonable time for the purpose for which it was being held, unless a law requires such data to be kept for a minimum time. Personal data that is no longer required will be destroyed or deleted in accordance with the Retention Schedule.

Individual Rights

Data subjects have the following rights in relation to their personal information:

- to be informed about how, why and on what basis the information is processed;
- to obtain confirmation that personal information is being processed and to obtain access to it and certain other information, by making a subject access request;
- to have data corrected if it is inaccurate or incomplete;
- to have data erased if it is no longer necessary for the purpose for which it was originally collected or processed;
- to restrict the processing of personal information where the accuracy of the information is contested;
- to receive or ask for, in limited circumstances, personal data to be transferred to a third party in a structured and commonly used format;
- to withdraw consent to processing at any time;
- to be notified of a data breach which may result in a high risk to their rights and obligations; and
- to make a complaint to the Information Commissioner's Office or a Court.

Individual Responsibilities

Staff may have access to the personal information of other members of staff, pupils or parents. Pushkin's School expects staff to help meet data protection obligations to those individuals.

Staff that have access to personal information must:

- only access the personal information if they have the authority to do so, and only for authorised purposes;
- only allow other staff to access personal information if they have appropriate authorisation;
- only allow individuals who are not school staff to access personal information if they have specific authority to do so;
- keep personal information secure;
- not remove personal information, or devices containing personal information, from the school's premises unless appropriate security measures are in place to secure the information and the device;
- not store personal information on local drives or on personal devices that are used for work purposes.

Information Security

Pushkin's School will use appropriate technical and organisation measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. The members of staff with access to the physical and electronic personal information are Elena Vlasenko (School Director), Olga Kisil (School Manager) and Anton Vlasenko (School Administrator).

Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Staff must exercise particular care in protecting sensitive data from loss or unauthorised access, use or disclosure. They must follow all procedures put in place to maintain the security of all personal data from the point of collection to the point of destruction.

Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the school implements and maintains in accordance with the GDPR and DPA. Staff must maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality – only people who have a need to know and are authorised to use the personal data can access it.
- Integrity – personal data is accurate and suitable for the purpose for which it is processed.
- Availability – authorised users can access the personal data when they need it for authorised purposes.

The school will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, identified risks and the amount of personal data it owns. The effectiveness of these safeguards will be evaluated regularly to ensure the security of processing.

Storage and Retention of Personal Information

Personal information on paper is stored in a locked filing cabinet outside school premises. Electronic personal information is stored on an encrypted and password-protected memory stick. A second encrypted memory stick is used as backup storage of personal information and will be located inside the locked filing cabinet.

Personal data will be kept securely in accordance with the school's data protection obligations and will not be retained for any longer than necessary. The length of time the data is retained will depend upon the circumstances, including the reasons why personal data was obtained. Personal information that is no longer required will be deleted in accordance with the school's Retention Schedule.

Data Breaches

A data breach may take many different forms:

- loss or theft of data or equipment on which personal information is stored;
- unauthorised access to or use of personal information by a member of staff;
- loss of data resulting from an equipment or systems failure;
- human error, such as accidental deletion or alteration of data;
- unforeseen circumstances, such as a fire or flood;
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams; or
- blagging offences where information is obtained by deceiving the organisation which holds it.

If the breach is likely to result in a risk to the rights and freedoms of the individual, Pushkin's School will report the breach to the Information Commissioner's Office within 72 hours. Staff must inform the School Director if a data breach is discovered and make all reasonable efforts to recover the information.

Training

Pushkin's School will ensure that all staff are adequately trained regarding their data protection responsibilities.

Consequences of a Failure to Comply

Pushkin's School takes compliance with this policy very seriously. Failure to comply puts data subjects whose personal information is processed at risk and carries the risk of significant civil and criminal sanctions for the individual and the school. In some circumstances, it could amount to a criminal offence by the individual.

Any failure to comply with this policy may lead to disciplinary action and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about this policy, you should contact the School Director (elena@pushkinsschool.co.uk) or the DPO (anton@pushkinsschool.co.uk).

Review of Policy

This policy will be updated as necessary to reflect best practice or the amendments made to the GDPR or DPA. It will also be reviewed annually by the DPO and approved by the School Director.

The Supervisory Authority in the UK

The Information Commissioner's Officer website (https://ico.org.uk) provides detailed guidance on a range of topics including individual's rights, data breaches, dealing with subject access requests and how to handle requests from third parties.