Data Protection Policy

Reviewed: **Sept 2020**
Review period: **2 yearly**
Review date: **Sept 2022**

Portesbery School
A happy school where every one matters

Data Protection Policy

1. Introduction and Purpose of Policy

The purpose of this policy is to provide information about our school's approach to collecting and using personal data in the course of our day-to-day work as well as the rights available to those whose data we hold.

It applies to personal data we collect both as an employer and as an education provider, such as that contained within pupil and staff records as well as information we hold on parents, governors, volunteers, visitors and other individuals with whom we interact.

The General Data Protection Regulation (GDPR) ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

2. Policy Statement

The Governing Body is committed to ensuring that personal data is collected and used in a way which is transparent, clearly understood and meets minimum legal requirements and best practice guidance. The Governing Body recognises the need for individuals to feel confident that their data will be used only for the purposes that they have been made aware of, and that it is stored securely and for no longer than is necessary. As part of this commitment, we want to ensure that individuals understand the rights available to them if they want to question or raise concerns about the way their data is being processed.

The School has appointed a Data Protection Officer whose role is to monitor internal compliance, including with this policy, to inform and advise on data protection obligations and act as a contact point for individuals and the Information Commissioner's Office.

Details of our Data Protection Officer can be found at the end of this policy document and requests for further information or queries relating to this policy can be sent directly to him.

3. Definitions and Principles

Certain terms are referred to in this policy which are explained below:

- **Personal data:** is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access.
- **Processing data:** involves any activity that involves the use of personal data. This includes but is not limited to: obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.
- **Special categories of personal data:** this refers to sensitive personal data, which includes information about an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, or sexual orientation.

- **Criminal offence data:** this includes data about criminal allegations, proceedings or convictions.
- **Data Protection Impact Assessment (DPIA)**
  DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.

Data protection principles to which the school must have regard when processing personal data.

These are that personal data shall be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- 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;
- Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed
- Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage
- The School will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. However, there may be circumstances where the School is required either by law or in the best interests of our pupils, parents or staff to pass information onto external authorities, for example, the local authority, Ofsted or the department of health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

4. Our Approach to Processing Personal Data

We use privacy notices to inform individuals whose personal data we collect about how we use their information and the legal basis on which we are processing it. If we want to process data for new reasons in the future, we will inform affected individuals first.

We process special categories of personal data and criminal offence data, for example to meet our obligations under employment law. Where we do so, this processing is underpinned by policies on the use of such data.

For some of the data we process we rely on legitimate interests as the legal basis for processing. We do not rely on this basis unless we have first concluded that the rights and freedoms of individuals do not override those interests.

Personal data we hold on individuals is held in secure paper and/or electronic files to which only authorised personnel have access. Information is held for no longer than is deemed necessary, in accordance with our data retention schedules and privacy notices.

If we are planning to process data and this processing is likely to result in a high risk to individuals' interests, we will undertake a Data Protection Impact Assessment (DPIA) to help us identify and minimise the data protection risks.

We always aim to rectify inaccurate or out-of-date information promptly when notified and encourage anyone whose data we hold to inform us when their details have changed.

5. Rights of Individuals

If we process your data you have a number of rights as an individual which are summarised below.

5.1 Right of access

You have the right to obtain confirmation from us that your data is being processed and to gain access to your personal data by making a subject access request. You should do this by emailing your request to data@portesbery.surrey.sch.uk or by post to the school's address. We are required to verify your identity before responding which may mean we ask you to provide identification documents. Parents may request information relating to their child. This will generally require the pupil's consent if the pupil is deemed competent to exercise his/her own rights.

In most cases we will respond to you within one calendar month of receipt. Please be aware that during closure periods we are unlikely to be able to deal with your request promptly so we ask that, wherever possible, you submit requests during term time.

We do not charge a fee for providing a copy of the information except where we have assessed the request as being manifestly unfounded or excessive or where further copies of the same information are asked for.

If we refuse to respond to a request we will explain why, as well as your right to complain to the Information Commissioner's Office.

Requests for education records: Where a parent has requested access to their child's educational record, this will be provided at no cost within 15 school days of receipt of the written request.

5.2 Other individual rights

In addition to the right of access described above, individuals have certain other rights. These are:

- **Right to rectification:** the right to have inaccurate personal data rectified, or completed if it is incomplete.
- **Right to erasure:** the right to have personal data erased (also known as the 'right to be forgotten').
- **Right to restrict processing:** the right to request the restriction or suppression of your personal data in certain circumstances.
- **Right to data portability:** the right in certain circumstances to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way.
- **Right to object:** the right to object to processing based on legitimate interests or the performance of a task in the public interest / exercise of official authority; this also covers direct marketing as well as processing for purposes of scientific or historical research and statistics.
- **Rights relating to automated decision making including profiling:** automated individual decision-making refers to making a decision solely by automated means without any human involvement; profiling refers to automated processing of personal data to evaluate certain things about an individual. We do not currently use automated decision making in any of our processing activities.

If you want to exercise any of these rights, you should do so by emailing your request to data@portesbery.surrey.sch.uk or by post to the school's address.

6. International Data Transfers

We do not transfer personal data to countries outside the EEA.

7. Our Approach to Data Security and Breaches

Our school is committed to ensuring that the personal data we hold and process is kept secure at all times and that data protection is considered and integrated into our processing activities. We use a variety of technical and organisational measures to protect personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or unauthorised access.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact Debbie Attard or your DPO. Reference should be made to the Data Breach policy.

In the event of a data breach taking place, we will report the circumstances to the Information Commissioner within 72 hours of becoming aware that it has occurred. We will also keep a register of data breaches that have occurred.

If a breach is likely to result in a high risk to the rights and freedoms of individuals, we will also inform those concerned directly and without undue delay.

8. Our Expectations of Staff

We expect all staff working for, or on behalf of, the school, whether employees, casual workers, supply staff, volunteers or consultants, to recognise and adhere to the high standards of data protection we uphold. Everyone has a responsibility for helping to ensure that personal data, whether their own or that of third parties, is accurate, kept up to date and held securely.

Certain members of staff will collect and process data as part of their role. Without exception we expect the following rules to be adhered to:

Members of staff must:

- Only access or process personal data they are authorised to as part of their role and in accordance with the documented purposes for processing (and not for any other purpose);
- Keep personal data confidential and only disclose it to individuals who are authorised to see it (if in any doubt, consulting their line manager or the Data Protection Officer);
- Not remove personal data from its authorised location without permission and, where permission is granted, to ensure that appropriate security measures are in place whilst the data is moved or relocated;
- Not keep work-related personal data on personal devices, such as mobile phones and tablets, or on local computer hard drives or unencrypted USB sticks;
- Take responsibility for ensuring that personal passwords are strong, are changed regularly and never shared;
- Adhere to all security measures designed to keep personal data safe from accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or unauthorised access;
- Participate in training or briefings and read circulated documents aimed at increasing awareness of data protection legislation and good practice;
- Be aware of data protection issues as part of their day-to-day work, particularly as part of any new projects, and report any concerns relating to personal data (including any potential data breaches) as a matter of urgency to the Data Protection Officer.

These rules are an integral part of the school's data security practices in order to comply with data protection legislation. As such, a breach of these rules is likely to be treated as a disciplinary offence and potentially gross misconduct, in accordance with the disciplinary procedure.

9. Privacy Notices

Privacy notices set out information for data subjects about how the School will use their data. Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we will provide the data subject with all the information required by the GDPR including the identity of the data protection officer, the School's contact details, how and why we will use, process, disclose, protect and retain personal data.

10. Data Impact Assessments

The School will conduct DPIAs for any new technologies or programmes being used by the School which could affect the processing of personal data.

11. Status of Policy and Review

The content and operation of this policy is reviewed as and when deemed necessary by the Governing Body or the Data Protection Officer. The policy is discretionary and does not confer any contractual rights.

Data Protection Officer Contact Details	
Name	**Craig Stilwell**
Organisation	**Judicium Consulting Ltd**
Email Address	**dataservices@judicium.com**
Telephone Number	**0203 326 9174**
Postal Address	**72 Cannon Street** **London EC4N 6AE**