THE PORTSMOUTH GRAMMAR SCHOOL

The PGS Data Protection Policy

Contents

1. Introduction

This Policy sets out the obligations of the School regarding data protection and the rights of, pupils, their parents, carers or guardians (referred to in this policy as "parents"), staff and visitors ("data subjects") in respect of their personal data under the Data Protection Act 2018 and the UK General Data Protection Regulation ("UK GDPR").

The UK GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"); 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.

This Policy sets out the School's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein are to be followed by the School, its employees, agents, contractors, or other parties working on behalf of the School.

The School is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2. The Data Protection Principles

This Policy aims to ensure compliance with the UK GDPR, which sets out the following principles with which any party handling personal data must comply. All personal data must be:

2.1 Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

2.2 Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. 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.

2.3 Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

2.4 Accurate and, where necessary, kept up to date. Every reasonable step is to be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.

2.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. 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 UK GDPR in order to safeguard the rights and freedoms of the data subject.

2.6 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.

3. The Rights of Data Subjects

The UK GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

3.1 The right to be informed;

3.2 The right of access;

3.3 The right to rectification;

3.4 The right to erasure (also known as the 'right to be forgotten');

3.5 The right to restrict processing;

3.6 The right to data portability;

3.7 The right to object; and

3.8 Rights with respect to automated decision-making and profiling.

4. Lawful, Fair, and Transparent Data Processing

4.1 The UK GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The UK GDPR states that processing of personal data shall be lawful if at least one of the following applies:

4.1.1 The data subject has given consent to the processing of their personal data for one or more specific purposes;

4.1.2 The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;

4.1.3 The processing is necessary for compliance with a legal obligation to which the School is subject;

4.1.4 The processing is necessary to protect the vital interests of the data subject or of another natural person;

4.1.5 The 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; or

4.1.6 The processing is necessary for the purposes of the legitimate interests pursued by the School or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

4.2 If the personal data in question is "special category data" (also known as "sensitive personal data"), for example, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation; at least one of the following conditions must be met:

4.2.1 The data subject has given their explicit consent to the processing of such data for one or more specified purposes;

4.2.2 The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the School or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by legislation which provides for appropriate safeguards for the fundamental rights and interests of the data subject);

4.2.3 The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

4.2.4 The processing is carried out in the course of the School's legitimate activities, provided that the processing relates solely to the members or former members of the School or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the School without the consent of the data subjects;

4.2.5 The processing relates to personal data which is clearly made public by the data subject;

4.2.6 The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;

4.2.7 The processing is necessary for substantial public interest reasons which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;

4.2.8 The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of current legislation, or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the UK GDPR;

4.2.9 The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of current legislation which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or

4.2.10 The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the UK GDPR, which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

5. Specified, Explicit, and Legitimate Purposes

5.1 The School collects and processes the personal data set out in Part 20 of this Policy. This includes:

5.1.1 Personal data collected directly from data subjects; and

5.1.2 Personal data obtained from third parties.

5.2 The School only collects, processes, and holds personal data for the specific purposes set out in Part 20 of this Policy (or for other purposes expressly permitted by the UK GDPR).

5.3 Data subjects are informed of the purpose or purposes for which the School uses their personal data. Please refer to Part 12 for more information on keeping data subjects informed.

6. Adequate, Relevant, and Limited Data Processing

The School will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 5, above, and as set out in Part 20, below.

7. Accuracy of Data and Keeping Data Up-to-Date

7.1 The School shall ensure that all personal data collected, processed, and held by it is kept accurate and up to date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 13, below.

7.2 The accuracy of personal data shall be checked when it is collected and if any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

8. Data Retention

8.1 The School shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

8.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

8.3 For full details of the School's approach to data retention, including retention periods for specific personal data types held by the School, please refer to The PGS Storage and Retention of Records and Documents Policy which is available on request.

9. Secure Processing

The School shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 21 to 28 of this Policy.

10. Accountability and Record-Keeping

10.1 The School has appointed the Bursar as the **Data Protection Lead** ("**DPL**") who will be responsible, with the Data Manager, for overseeing the implementation of this Policy, the School's other data protection-related policies, and the UK GDPR and other applicable data protection legislation, and will endeavour to ensure that all personal data is processed in compliance with this policy and current legislation.

10.2 The School has also appointed an external **Data Protection Officer** ("**DPO**"). This is GDPR Sentry, Unit 434 Birch Park, Thorp Arch Trading Estate, Wetherby, LS23 7FG, who can be contacted on 0113 804 2035, or support@gdprsentry.com

10.3 The Data Protection Officer has an advisory role in relation to this Policy, the School's other data protection-related policies, and with the UK GDPR and other applicable data protection legislation.

10.4 The School shall keep written internal records of all personal data collection, holding, processing, and for how long it will be retained.

11. Data Protection Impact Assessments

11.1 The School shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the UK GDPR.

11.2 Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

11.2.1 The type(s) of personal data that will be collected, held, and processed;

11.2.2 The purpose(s) for which personal data is to be used;

11.2.3 The School's objectives;

11.2.4 How personal data is to be used;

11.2.5 The parties (internal and/or external) who are to be consulted;

11.2.6 The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

11.2.7 Risks posed to data subjects;

11.2.8 Risks posed both within and to the School; and

11.2.9 Proposed measures to minimise and handle identified risks.

12. Data Subject Access

12.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the School holds about them, what it is doing with that personal data, and why. Pupils can make subject access requests for their own personal data, provided that, in the reasonable opinion of the School, they have sufficient maturity to understand the request they are making. Pupils aged 12 or over are generally assumed to have this level of maturity, although this will depend on both the child and the personal data requested. All subject access requests from pupils will therefore be considered on a case by case basis.

12.2 Data subjects wishing to make a SAR should usually contact the School's Data Protection Lead, the Bursar, in the first instance.

12.3 Responses to SARs shall normally be made within one month of receipt; however this may be extended by up to two further months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

12.4 Responses to SARs shall be dependent upon the terms of the UK GDPR, the Data Protection Act (2018) and associated ICO guidance.

12.5 The School does not usually charge a fee for the handling of SARs. The School reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

13. Rectification of Personal Data

13.1 Data subjects may have the right to require the School to rectify any of their personal data that is inaccurate or incomplete.

13.2 Where such rectification is possible, the School shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the School of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

13.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

14. Erasure of Personal Data

14.1 Data subjects have the right to request that the School erases the personal data it holds about them in the following circumstances:

14.1.1 It is no longer necessary for the School to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;

14.1.2 The data subject wishes to withdraw their consent to the School holding and processing their personal data;

14.1.3 The data subject objects to the School holding and processing their personal data (and there is no overriding legitimate interest to allow the School to continue doing so) (see Part 17 of this Policy for further details concerning the right to object);

14.1.4 The personal data has been processed unlawfully;

14.1.5 The personal data needs to be erased in order for the School to comply with a particular legal obligation; or

14.1.6 The personal data is being held and processed for the purpose of providing information society services to a child.

14.2 Unless the School has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

14.3 In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

15. Restriction of Personal Data Processing

15.1 Data subjects may request that the School restricts processing the personal data it holds about them. If a data subject makes such a request, the School shall in so far as is possible ensure that the personal data is only stored and not processed in any other fashion.

15.2 If the School is required to process the data for statutory purposes or for reasons of legal compliance, then the School shall inform the Data Subject that this processing is expected to take place. If possible, this notice will be provided prior to processing.

15.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

16. Data Portability

16.1 The School processes personal data using automated means. Such processing is carried out for example by our management information system, our human resources system, our injury reporting system and our catering management system.

16.2 Where data subjects have given their consent to the School to process their personal data in such a manner, or the processing is otherwise required for the normal operation of the School, data subjects have the right, under the UK GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

17. Objections to Personal Data Processing

17.1 Data subjects have the right to object to the School processing their personal data based on legitimate interests or direct marketing (including profiling)

17.2 Where a data subject objects to the School processing their personal data based on its legitimate interests, the School shall cease such processing immediately, unless it can be demonstrated that the School's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

17.3 Where a data subject objects to the School processing their personal data for direct marketing purposes, the School shall cease such processing immediately.

17.4 Where a data subject objects to the School processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the UK GDPR, "demonstrate grounds relating to his or her particular situation". The School is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

18. Automated Decision-Making

The School is not currently using personal data in automated decision-making processes.

19. Profiling

The School uses personal data for profiling purposes. These purposes relate to helping pupils maximise achievement and attendance. All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling.

20. Personal Data Collected, Held, and Processed

The School uses a wide range of personal data across many processes. More detail can be found in our privacy notices. If you wish to view the complete lists of categories of personal data we process please contact our DPL.

21. Data Security - Transferring Personal Data and Communications

The School shall ensure that the appropriate measures are taken with respect to all communications and other transfers involving personal data:

21.1 Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

21.2 The School will ensure that where special category personal data or other sensitive information is sent in the post that it shall be possible to demonstrate that it was delivered.

21.3 Where special category personal data or other sensitive information is to be sent by e-mail the email will either be sent using a suitable encryption method or the data will be sent in an attached, encrypted document and not in the body of the e-mail.

21.4 Where personal data is to be transferred in removable storage devices, these devices shall be encrypted. The use of unencrypted removable storage devices is prohibited by the School

22. Data Security - Storage

The School shall ensure that the following measures are taken with respect to the storage of personal data:

22.1 All electronic copies of personal data should be stored securely using passwords, user access rights and where appropriate data encryption;

22.2 All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;

22.3 All personal data relating to the operations of the School, stored electronically, should be backed up on a regular basis

22.4 Where any member of staff stores personal data on a mobile device (whether that be computer, tablet, phone or any other device) then that member of staff must abide by the Acceptable Use policy of the School. The member of staff shall also ensure that they can provide a secure environment for that device to be used to minimise any risk to the confidentiality or integrity of the information

23. Data Security - Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to The PGS Storage and Retention of Records and Documents Policy.

24. Data Security - Use of Personal Data

The School shall ensure that the following measures are taken with respect to the use of personal data:

24.1 No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the School requires access to any personal data that they do not already have access to, such access should be formally requested from the Bursar;

24.2 Personal data must always be handled with care and should only be shared on a 'need to know' basis[1] and must not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;

24.3 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and

24.4 Where personal data held by the School is used for marketing purposes, the School will ensure that the appropriate consent has been obtained.

25. Data Security - IT Security

The School shall ensure that the following measures are taken with respect to IT and information security:

[1] Of note, for example, student fee assistance is personal data and should not be shared outside the admissions and bursary teams without an explicit requirement to do so.

25.1 The School requires that any passwords used to access personal data shall have a minimum of 8 characters, composed of a mixture of upper- and lower-case characters, numbers and symbols, or as agreed in writing from time to time by the Information Services Programme Board (ISPB). Passwords are not expected to be changed upon a regular basis, but users will be expected to change their password if instructed by the School;

25.2 Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the School, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

25.3 All software (including, but not limited to, applications and operating systems) shall be kept up to date. The School's IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so;

25.4 No software may be installed on any School-owned computer or device without the prior approval of the Head of ICT Services; and

25.5 Where members of staff or other user use online applications that require the use of personal data, the use of that application must be approved/signed off by the Head of ICT Services.

26. Organisational Measures

The School shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

26.1 All employees, agents, contractors, or other parties working on behalf of the School shall be made fully aware of both their individual responsibilities and the School's responsibilities under the UK GDPR and under this Policy, and shall have free access to a copy of this Policy;

26.2 Only employees, agents, sub-contractors, or other parties working on behalf of the School that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the School;

26.3 All employees, agents, contractors, or other parties working on behalf of the School handling personal data will be appropriately trained to do so, appropriately supervised and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

26.4 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

26.5 The contravention of these rules will be treated as a disciplinary matter;

26.6 All employees, agents, contractors, or other parties working on behalf of the School handling personal data will be bound to do so in accordance with the principles of the UK GDPR and this Policy;

26.7 All agents, contractors, or other parties working on behalf of the School handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the School arising out of this Policy and the UK GDPR; and

26.8 Where any agent, contractor or other party working on behalf of the School handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the School against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

27. Transferring Personal Data to a Country Outside the EEA

27.1 The School may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

27.2 Should the transfer of personal data to a country outside of the EEA take place, the School will ensure that it meets the requirements of current legislation.

28. Data Breach Notification

28.1 All personal data breaches must be reported immediately to the School's Data Protection Lead, and where necessary to the DPO.

28.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the DPL must ensure the DPO is informed of the breach as soon as possible, and no later than 24 hours after the breach has been discovered; the DPO will support the School with any investigation, write an appropriate report and, with the DPL, ensure that the Information Commissioner's Office is informed within 72 hours after the DPL has become aware of it.

28.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 28.2 above) to the rights and freedoms of data subjects, the DPO must ensure that all affected data subjects are informed of the breach directly and without undue delay.

29. Queries and complaints

If you have any comments or queries on this policy, we recommend that in the first instance you direct these to the School's Data Protection Lead, the Bursar.

Alternatively, you can contact the School's appointed Data Protection Officer:

Name of DPO:	GDPR Sentry Limited
Email address:	support@gdprsentry.com
Contact number:	0113 804 2035
Contact address:	Unit 434, Birch Park, Thorp Arch Trading Estate, Wetherby, LS23 7FG

Allocation of Tasks and Version control

Allocation of Tasks

Task	Allocated to	When / frequency of review
Keeping the policy up to date and compliant with the law and best practice	DPL	As required, and at least annually
Monitoring the implementation of the policy, relevant risk assessments and any action taken in response and evaluating effectiveness	DPL	As required, and at least termly
Maintaining up to date records of all information created in relation to the policy and its implementation as required by the UK GDPR	Head of ICT Services	As required, and at least termly
Receiving / reviewing input from interested groups (such as pupils, staff, Parents) to consider improvements to the School's processes under the policy	Information Services Programme Board	As required, and at least annually
Formal annual review	Senior Management Team	Annually

Version Control

Date Approved	26th June 2024 (Senior Management Team) (updated 4-9-24)
Date Reviewed	20th June 2024 (IPSB) (em)
Next Review Date	Summer Term 2025
Policy author (SMT)	Bursar
Status	External
Report	ICT and Data Report

Ph4040924