PURBROOK JUNIOR SCHOOL

DREAM BIG!

Respect - Team - Achieve

Data Protection Policy (including Data Breach Policy)

Policy Number:	SP9	**Created by:**	HCC Model Policy (last updated January 2021)
Reviewed by:	Data Protection Officer	**Responsibility:**	Resources Committee
Last Review:	Summer 2024	**Next Review:**	Summer 2026
Review Cycle:	Two Years	**Ratified by GB:**	15/07/2024

This policy is available in large print. Please contact the school office who will be happy to arrange this for you.

The school collects and uses personal information (referred to in the UK General Data Protection Regulation (UK GDPR) as personal data) about staff, pupils, parents and 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. In addition, the school may be required by law to collect, use and share certain information.

The school is the Data Controller, of the personal data that it collects and receives for these purposes.

Purbrook Junior School's Data Protection Officer is Mrs Helen Saunders, School Business Manager, who can be contacted via the school office.

The school issues Privacy Notices (also known as a Fair Processing Notices) to all pupils/parents and staff. These summarise the personal information held about pupils and staff, the purpose for which it is held and who it may be shared with. It also provides information about an individual's rights in respect of their personal data.

Purpose

This policy sets out how the school deals with personal information correctly and securely and in accordance with the UK GDPR, and other related legislation.

This policy applies to all personal information however it is collected, used, recorded and stored by the school and whether it is held on paper or electronically.

What is Personal Information/ data?

Personal information or data means any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified, directly or indirectly by reference to details such as a name, an identification number, location data, an online identifier or by their physical, physiological, genetic, mental, economic, cultural or social identity. Personal data includes (but is not limited to) an individual's, name, address, date of birth, photograph, bank details and other information that identifies them.

Data Protection Principles

The UK GDPR establishes six principles as well as a number of additional duties that must be complied with at all times:

1. **Lawfulness, fairness and transparency.** Personal data shall be processed lawfully, fairly and in a transparent manner. In order for personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the UK GDPR. These include (amongst other relevant conditions) where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority exercised by the school. Where the special categories of personal data are processed, this shall include (amongst other relevant conditions) where processing is necessary for reasons of substantial public interest. When processing personal data and special category data in the course of school business, the school will ensure that these requirements are met where relevant.
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 (subject to exceptions for specific archiving purposes). The school will only process personal data for specific purposes and will notify those purposes to the data subject when it first collects the personal data or as soon as possible thereafter.
3. **Data minimisation**. Personal data shall be adequate, relevant and limited to what is necessary to the purposes for which they are processed and not excessive. Personal data which is not necessary for the purpose for which it is obtained will not be collected.
4. **Accuracy.** Personal data shall be accurate and where necessary, kept up to date; Personal data should be reviewed and updated as necessary and should not be retained unless it is reasonable to assume that it is accurate. Individuals should notify the school of any changes in circumstances to enable records to be updated accordingly. The school will be responsible for ensuring that updating or records takes place where appropriate.
5. **Storage limitation.** Personal data shall be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. The school will not keep personal data for longer than is necessary for the purpose or purposes for which they were collected and will take reasonable steps to destroy or erase from its systems all data which is no longer required.
6. **Integrity and confidentiality**. Personal data shall be processed in a manner that ensures appropriate security of the personal data and which includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Duties

Personal data shall not be transferred to a country or territory outside the UK and the European Union (EU)/European Economic Area (EEA), unless that country or territory ensures an adequate level of data protection.

Data Controllers have a General Duty of accountability for personal data.

Commitment

Purbrook Junior School is committed to maintaining the principles and duties in the UK GDPR at all times. Therefore the school will:

- Inform individuals of the identity and contact details of the data controller.
- Inform individuals of the contact details of the Data Protection Officer
- Inform individuals of the purposes that personal information is being collected and the basis for this.
- Inform individuals when their information is shared, and why and with whom unless the UK GDPR provides a reason not to do this.
- If the school plans to transfer personal data outside the UK and the EU/EEA the school will inform individuals and provide them with details of where they can obtain details of the safeguards for that information.
- Inform individuals of their data subject rights.
- Inform individuals that the individual may withdraw consent (where relevant) and that if consent is withdrawn that the school will cease processing their data although that will not affect the legality of data processed up until that point.
- Provide details of the length of time an individual's data will be kept

- Should the school decide to use an individual's personal data for a different reason to that for which it was originally collected the school shall inform the individual and where necessary seek consent.
- 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 UK and the EU/EEA without the appropriate safeguards.
- Ensure that all staff and governors are aware of and understand these policies and procedures.

Retention and Disposal of Personal Data

Purbrook Junior School will dispose of personal data in a way which protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) as appropriate.

Purbrook Junior School maintains a Retention Schedule that is specific and relevant to the specific types of information retained. The schedule outlines the appropriate periods for retention in each case.

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 at Wycliffe House, Water Lane Wilmslow Cheshire SK9 5AF or at www.ico.gov.uk

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 Data Protection Officer, Headteacher, or nominated representative.

Contacts

If you have any enquires in relation to this policy, please contact Mrs H Saunders, Data Protection Officer for Purbrook Junior School.

Appendix A

Schedule 1, Part 4, Data Protection Act 2018: Appropriate Policy Document

Processing special category data & criminal offence data based on substantial public interest conditions & the employment, social security & social protection condition

As part of the School's statutory and administrative functions, we process special category data and (where relevant) criminal offence data in accordance with the requirements of Article 9 and 10 UK General Data Protection Regulation ('UK GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

Some of the Schedule 1 conditions for processing special category and criminal offence data require us to have an appropriate policy document (APD) in place, setting out and explaining our procedures for securing compliance with the data protection principles in Article 5 UK GDPR and policies regarding the retention and erasure of such personal data.

This document is the Schedule 1, Part 4, DPA 2018 Appropriate Policy Document for the School which should be read alongside the School's Data Protection Policy.

1. Definitions

Special category data is information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Criminal conviction data is information relating to criminal convictions and offences or related security measures and this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data'.

Processing which requires an Appropriate Policy Document
The following Schedule 1 conditions require an APD:

- employment, social security and social protection condition[1]
- substantial public interest conditions[2]

This document demonstrates that the processing of special category data and criminal offence data based on these specific Schedule 1 conditions is compliant with the requirements of the data protection principles and outlines our retention policies with respect to this data.

2. Description of data processed

We process special category data about our employees that is necessary to fulfil our obligations as an employer. This includes information about their health and wellbeing, ethnicity, and their membership of any trade union. We process criminal offence data about job applicants and our employees that is necessary to fulfil our obligations as an employer and legal obligations. We process special category data as an employer for reasons of substantial public interest for purposes of equality of opportunity or treatment monitoring and promoting racial and ethnic diversity in the organisation.

We process special category data (and criminal offence data) about individuals for reasons of substantial public interest to fulfil our statutory functions e.g. the keeping and maintaining of pupil records as well as safeguarding and promoting the welfare of pupils.

Further information about this processing can be found on the school's Privacy Notice.

3. Schedule 1 conditions for processing (which require an APD)

[1] Paragraph 1 of Part 1 of Schedule 1 to the DPA 2018

[2] All the substantial public interest conditions in Part 2 of Schedule 1 to the DPA 2018 require an APD to be in place except for in the specified circumstances outlined in the preventing or detecting unlawful acts condition (paragraph 10), journalism etc in connection with unlawful acts and dishonesty etc condition (paragraph 13) and anti-doping in sport condition (paragraph 27).

Special category data

The School may process special category data under the following conditions in Part 1 and Part 2 of Schedule 1:

- Employment, social security and social protection (paragraph 1)
- Statutory and government purposes (paragraph 6)
- Equality of opportunity or treatment (paragraph 8)
- Racial and ethnic diversity at senior levels of organisation (paragraph 9)
- Preventing or detecting unlawful acts (paragraph 10)
- Protecting the public against dishonesty (paragraph 11)
- Regulatory requirements relating to unlawful acts and dishonesty (paragraph 12)
- Counselling etc (paragraph 17)
- Safeguarding of children and of individuals at risk (paragraph 18)
- Occupational pensions (paragraph 21)
- Disclosure to elected representatives (paragraph 24)

4. Criminal offence data

The School may process criminal offence data under the following conditions in Parts 1 and 2 of Schedule 1:

- Employment, social security and social protection (paragraph 1)
- Statutory and government purposes (paragraph 6)
- Preventing or detecting unlawful acts (paragraph 10)
- Protecting the public against dishonesty (paragraph 11)
- Regulatory requirements relating to unlawful acts and dishonesty (paragraph 12)
- Safeguarding of children and of individuals at risk (paragraph 18)

5. Compliance with the data protection principles

The School's procedures for ensuring compliance with the principles are detailed below:

Accountability principle

We have put in place appropriate technical and organisational measures to meet the requirements of accountability[3]. These include:

- The appointment of a data protection officer who reports directly to our highest management level.
- Taking a 'data protection by design and default' approach to our activities.
- Maintaining documentation of our processing activities.
- Adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors.
- Implementing appropriate security measures in relation to the personal data we process.
- Carrying out data protection impact assessments for our high-risk processing.

We regularly review our accountability measures and update or amend them when required.

Principle (a): lawfulness, fairness and transparency

Processing personal data must be lawful, fair and transparent. It is only lawful if and to the extent it is based on law and either the data subject has given their consent for the processing, or the processing meets at least one of the conditions in Schedule 1 of the DPA 2018.

We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notices, staff privacy notice and this policy document.

Our processing for purposes of substantial public interest is necessary for the exercise of statutory functions.
We have responsibilities under the law to safeguard children and individuals at risk.

Our processing for the purposes of employment relates to our obligations as an employer.

We also process special category personal data to comply with other obligations imposed on the School e.g. the Education Act 2002.

[3] The school should check and delete any of these which do not apply to their school, you should also add any other technical and organisational measures that you consider appropriate.

Principle (b): purpose limitation
We process personal data for purposes of substantial public interest as explained above when the processing is necessary for us to fulfil our statutory functions, where it is necessary for complying with or assisting another to comply with a regulatory requirement to establish whether an unlawful or improper conduct has occurred or to protect the public from dishonesty.

We are authorised by law to process personal data for these purposes. We may process personal data collected for any one of these purposes (whether by us or another controller), for any of the other purposes here, providing the processing is necessary and proportionate to that purpose.

If we are sharing data with another controller, we will document that they are authorised by law to process the data for their purpose.

We will not process personal data for purposes incompatible with the original purpose it was collected for.

Principle (c): data minimisation
We collect personal data necessary for the relevant purposes and ensure it is not excessive. The information we process is necessary for and proportionate to our purposes.

Principle (d): accuracy
Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights do not apply, we will document our decision.

Principle (e): storage limitation
All special category data and criminal offence data processed by us for the purpose of employment or substantial public interest is retained for the periods set out in the School's retention schedules. Our retention periods for this data are based on our legal obligations and the necessity of its retention for our business needs. Our retention schedules are reviewed regularly and updated when necessary.

Principle (f): integrity and confidentiality (security)
Electronic information is processed within our secure network. Hard copy information is processed in line with our security procedures for paper documents.

Our electronic systems and physical storage have appropriate access controls applied.

6. Retention and erasure policies

Our retention and erasure practices are set out in the retention schedules for our services, copies of which are available on request.

7. APD review date

This policy will be retained for the duration of our processing and for a minimum of 6 months after processing ceases. This policy will be reviewed every two years or revised more frequently if necessary.

8. Additional special category processing

We process special category personal data in other instances where it is not a requirement to keep an appropriate policy document. Our processing of such data respects the rights and interests of the data subjects. We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notices. Further information on all our processing can be found in our Data Protection Policy.

Appendix B

DATA BREACH POLICY

1. Introduction

This is the school's Data Breach policy which should be read alongside our Data Protection Policy.

To carry out the school's functions it is necessary to process personal data relating to our staff, pupils, parents, visitors and others.

Personal data is information relating to a living individual who:

- can be identified or who are identifiable, directly from the information in question; or
- who can be indirectly identified from that information in combination with other information.

The personal data the school processes includes special category data this is data which is of sensitive nature such as health information, racial or ethnic origin, biometric data and trade union membership.

2. What is a Personal Data Breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

3. What responsibilities does the school have in relation to a personal data breach?

3.1 Notification to the ICO

The school is required by the GDPR to report certain types of personal data breach to the Information Commissioner's Office (ICO).

When a personal data breach has occurred, the school will need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's **likely** that there will be a risk, then the school must notify the ICO; if it's unlikely then the school doesn't have to report it.

The school must report a notifiable breach to the ICO within 72 hours of becoming aware of the breach, where feasible.

3.2 Communication with the affected individuals

The school is required by the GDPR to inform the affected individual(s) of certain types of personal data breach.

If a breach is likely to result in a **high risk** to the rights and freedoms of individuals, the GDPR requires the school to inform those concerned directly and without undue delay i.e. as soon as possible.

In addition to informing the individual about the nature of the personal data breach the school must provide them with information about:

- The name and contact details of our DPO for any queries
- The likely consequences of the personal data breach
- The measures taken/to be taken to address the breach including where appropriate measures to mitigate the possible adverse effects

The school might not be required to notify the affected individual if certain exceptions apply.

3.3 Record keeping

The school will keep a record of any personal data breaches whether they are notifiable to the ICO or not including the facts of the personal data breach, its effects and the remedial action taken.

4. School's processors

Some of the school's contractors e.g. our IT suppliers process personal data on behalf of the school. The GDPR requires our contractors processing data on our behalf to notify the school without undue delay after becoming aware of a personal data breach. Our processors are required by the terms and conditions of their contracts to assist the School with any personal data breaches.

5. The School's procedures

The school has appropriate data breach procedures in place for our staff which deal with:

- reporting data protection incidents
- investigating data protection incidents
- managing data protection incidents
- containing and/or recovering data
- assessing the risk
- notification to the ICO/individual
- recording data protection incidents and action taken

6. Training

Our staff are provided with data protection training (which includes guidance on personal data breaches) and information on how to report a data protection incident and the school's policies and procedures relating to data protection and personal data breaches.

7. Review

This policy will be reviewed annually and updated as required.

8. Contact

Mrs H Saunders, the School's Data Protection Officer (023 9225 4577 or adminoffice@purbrook-jun.hants.sch.uk) can be contacted with any queries about this policy.