Pirton Hill Primary School

Data Protection Policy

Ratified by Governors: March 2025
Review date: July 2027

Overarching Values

Expect:
*We all **expect** to work hard, and meet our own high expectations, in a safe environment with access to high quality resources and opportunities that broaden our horizons.*

Believe:
*We all **believe** in ourselves, and each other, and know that everyone has something special to contribute.*

Achieve:
*We all have the opportunity to **achieve**, and fulfil our potential, regardless of our backgrounds.*

Enjoy:
*We all strive to develop passionate and determined life-long learners who **enjoy** learning, understand how to progress and take pleasure in succeeding.*

1 Introduction

Our School aims to ensure that all personal data collected about staff, pupils, parents and carers, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

This policy has been developed to ensure all staff, contractors and partners understand their obligations when processing personal and special category data.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2 Legislation and Guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020

- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

It also reflects the ICO's guidance for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3 The Data Controller

Our School processes personal data relating to parents and carers, pupils, staff, governors, visitors and others, and therefore is a Data Controller.

Our School is registered with the Information Commissioners Office (ICO), as legally required.

4 Roles and Responsibilities

This policy applies to all staff employed by our School, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Governing Body

The governing board has overall responsibility for ensuring that our School complies with all relevant data protection obligations.

Data Protection Officer (DPO)

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable, processing Subject Access Requests (SARs) and Freedom of Information Requests (FOIs), investigating data breaches and liaising with ICO.

They will provide a termly report of their activities directly to the Governing Body.

The DPO is also the first point of contact for individuals whose data the School processes, and for the ICO.

Our DPO is the School Business Manager and is contactable via businessmanager@pirtonhill.co.uk

Headteacher

The Headteacher acts as the representative of the data controller on a day-to-day basis.

All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy;
- Adhering to the Data Protection principles (section 5);
- Complying with the 'prohibited activities' (Section 18);
- Informing the school of any changes to their personal data, such as a change of address;
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure;
    - If they have any concerns that this policy is not being followed;

- If they are unsure whether or not they have a lawful basis to use personal data in a particular way;
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK;
- If there has been a data breach;
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals;
- If they need help with any contracts or sharing personal data with third parties.

5 Data Protection Principles

The UK GDPR is based on data protection principles that our School must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
- 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 ('purpose limitation');
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are 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 GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
- 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 ('integrity and confidentiality').".

This policy sets out how our School aims to comply with these principles.

6 Collecting Personal Data

Lawfulness, fairness and transparency

We will only process personal data where we have 1 of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the School can fulfil a contract with the individual, or the individual has asked the School to take specific steps before entering into a contract;

- The data needs to be processed so that the School can comply with a legal obligation;
- The data needs to be processed to ensure the vital interests of the individual or another person i.e. to protect someone's life;
- The data needs to be processed so that the School, as a public authority, can perform a task in the public interest or exercise its official authority;
- The data needs to be processed for the legitimate interests of the School (where the processing is not for any tasks the School performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden;
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent.

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given explicit consent;
- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law;
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent;
- The data has already been made manifestly public by the individual;
- The data needs to be processed for the establishment, exercise or defence of legal claims;
- The data needs to be processed for reasons of substantial public interest as defined in legislation;
- The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law;
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given consent
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights

- The data needs to be processed for reasons of substantial public interest as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

Limitation, minimisation and accuracy
We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons through our Privacy Notices.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the School's record retention schedule.

7 Sharing Personal Data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk;
- We need to liaise with other agencies – we will seek consent as necessary before doing this;
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors that can provide sufficient guarantees that they comply with UK data protection law;
    - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share;
    - Only share data that the supplier or contractor needs to carry out their service.

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

8 Sending Data Securely

We will send documents containing personal data securely using the following methods:

Requested by:	Method:
Hard copy	Documents should be hand delivered to the authorised recipient wherever possible. Make sure that the documents are securely contained in a sealed envelope. If it not possible for the data subject to collect the documents themselves use the **special or recorded delivery service**. **Note**: Check you have the correct address before posting
Email	**This is the preferred method**. Scan a copy of the file and move it to a secure location on the school's network. Send the file by secure data transfer [currently Egress]. Ask the data subject to confirm receipt of the documents as soon as possible

9 Subject Access Requests and Other Rights of Individuals

Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed;
- Access to a copy of the data;
- The purposes of the data processing;
- The categories of personal data concerned;
- Who the data has been, or will be, shared with;
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period;
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing;
- The right to lodge a complaint with the ICO or another supervisory authority;
- The source of the data, if not the individual;
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual;
- The safeguards provided if the data is being transferred internationally.

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address

- Details of the information requested

If staff receive a subject access request in any form they must immediately inform the DPO.

Children and subject access requests
Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Responding to subject access requests
When responding to requests, we:

- May the individual to provide a form of photographic identification;
- May contact the individual via phone to confirm the request was made;
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant);
- Will provide the information free of charge;
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual;
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests;
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it;
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

10 Other Data Protection Rights of the Individual

In addition to the right to make a subject access request, and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time;
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances);
- Prevent use of their personal data for direct marketing;
- Object to processing that has been justified on the basis of public interest, official authority or legitimate interests;
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement);
- Be notified of a data breach (in certain circumstances);
- Make a complaint to the ICO;
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

11 Parental Requests to See the Educational Record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

12 CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the Headteacher.

13 Photographs and Videos

As part of our school activities, we may take photographs and record images of individuals within our School.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and the pupil.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Where the School takes photographs and videos, uses may include:

- Within school on notice boards and in school newsletters, etc;
- Outside of school by external agencies such as the school photographer, newspaper;
- Online on our school website or social media pages.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

14 Artificial Intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. School recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, we will treat this as a data breach, and will follow the personal data breach procedure outlined in our Data Breach policy.

15 Data Protection by Design and Default

Under the Data Protection Act 2018, the School has a general obligation to implement technical and organisational measures to show that we have considered and integrated data protection into our processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge;
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 4)'
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will assist with this process);
- Integrating data protection into internal documents including this policy, any related policies and privacy notices;

- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance and training;
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant;
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply.
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO, and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

16 Privacy Impact Assessments

Staff are expected to complete Privacy Impact Assessments (PIA) to help identify and minimise any data protection risks.

A PIA is required for certain types of processing, or any other processing that is likely to result in a high risk to individuals' interests. It is good practice to do a PIA for any major project which requires the processing of personal data.

A PIA must:

- Describe the nature, scope, context and purposes of the processing;
- Assess necessity, proportionality and compliance measures;
- Identify and assess risks to individuals; and
- Identify any additional measures to mitigate those risks.

To assess the level of risk, you must consider both the likelihood and the severity of any impact individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

Staff should refer to the Data Protection Impact Assessment Guidance and consult the DPO where necessary.

17 Data Security and Storage of Records

Keeping personal data secure is vital in complying with the Data Protection Act. All staff, contractors and third parties are responsible for ensuring that personal data is kept secure and is not disclosed inappropriately (in any form) to unauthorised third parties.

School will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Keep passwords safe and never share them;
- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use;
- Papers containing confidential personal data must not be left unattended on office and classroom desks, on staffroom tables, or left anywhere else where there is general access;
- Consider of it is necessary to take hard copies of personal information off site at all, or if so, take the information on an encrypted device.
- Where hard copies of personal information need to be taken off site, ensure that those documents (including notebooks and files) are kept secure and looked after at all times.
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites;
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment;
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

18 Prohibited Activities

The following activities are strictly prohibited when processing personal and special category data:

- Sharing passwords to access data;
- Sending personal data to a personal email address to work on at home;
- Sending data to unauthorised personnel. Always check that the recipients are authorised to view the information being sent;
- Sending personal data in an unsecure format;
- Leaving personal data unprotected;
- Accessing information about a pupil or member of staff where there is no legitimate reason for doing do;
- Accessing personal data about an individual for personal use;
- Disclosing personal data to a third person outside of the School without a lawful basis.

19 Retention and Disposal of Records

School will retain information for the required length of time as stipulated by the relevant legislation, and/or 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.

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Refer to the Retention and Disposal policy.

20 Personal Data Breaches

The School will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in our Data Breach policy.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it.

Refer to the Data Breach policy.

21 Training

All staff are required to undertake an online data protection training as part of their induction process and complete an annual refresher course through SmartLog.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

22 Implications of Breaching this Policy

It is a condition of employment in the case of staff and contractors that they abide by the law and the policies of the School. Any breach of this policy could be considered to be a disciplinary offence and may lead to disciplinary action. A serious breach of the Data Protection Act may also result in the school and/or the individual being held liable in law.

23 Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed every two years and approved by the Resources Committee.

24 Links with Other Policies

This data protection policy is linked to our:

- Data Breach policy;
- Subject Access Requests policy;
- Subject Access Request procedure;
- Freedom of Information policy;
- Retention and Disposal policy.

Appendix 1 - Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

TERM	DEFINITION
Subject Access Request (SAR)	A request for access to data by a living person under the Act is known as a Subject Access Request or SAR. All records that contain the personal data of the subject will be made available, subject to certain exemptions.
Freedom of Information (FOI)	A request for access to data by a living person under the FOI Act. Freedom of a person or people to publish and have access to information about the activities of public authorities.
Lawful Basis	The grounds specified by the Regulations which need to be satisfied for any data processing to be legal. One ground needs to exist for processing personal data. Where special category data is processed a second ground must also exist.