



## Pirton Hill Primary School

### Subject Access Request Policy and Procedure

Ratified by Governors: June 2025

Review date: Summer 2028

#### 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.*

#### Introduction

The General Data Protection Regulation and The Data Protection Act 2018 (the Act) gives individuals certain rights over the use, the processing and access to their personal data held by the School. One of the rights enables individuals to find out what personal data is held, why it is held and who it is disclosed to. This right, is commonly known as 'subject access' and is set out in Article 15 of the GDPR. Individual may exercise the right by making a 'subject access request' (SAR).

The School is committed to upholding its responsibilities under the data protection legislation and respects the rights of data subjects.

The aim of this policy is to ensure that the school complies with its legal obligations under GDPR and the Data Protection Act 2018. It also aims to ensure that we:

- Have robust processes in place for dealing with SARs, saving time and effort;
- Increase levels of trust and confidence by being open with individuals about the personal information we hold;
- Improve the transparency of our activities in line with public policy requirements.

## Definitions

<b>Subject Access Request or SAR</b>	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.
<b>Freedom of Information Request or FOI.</b>	A request for access to data held is dealt with under the Freedom of Information Act 2000 and is known as a Freedom of Information Request or FOI. Requests for the data of deceased people may be processed under this legislation.
<b>Personal Data</b>	Personal data means data which relates to a living individual who can be identified directly or indirectly from the data, particularly by reference to an identifier. Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).
<b>Special Category Data</b>	Certain personal data, special category data, is given special protections under the Act because misuse could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination. Special category data includes: <ul style="list-style-type: none"> <li>• a person's racial or ethnic origin;</li> <li>• political opinions;</li> <li>• religious or similar beliefs;</li> <li>• trade union membership;</li> <li>• physical or mental health or condition or sexual life;</li> <li>• biometric or genetic data.</li> </ul>
<b>Data Controller</b>	The organisation which determines the purposes and the manner in which, any personal data is processed is known as the data controller. The school is the data controller of all personal data used and held within each part of the school
<b>Data Processors</b>	Organisations or individuals who process personal data on behalf of a data controller are known as data processors. Employees of data controllers are excluded from this definition, but it could include suppliers which handle personal data on our behalf.
<b>Data Subject</b>	A living individual who is the subject of personal data is known as the data subject. This need not be a UK national or resident. Provided that the data controller is subject to the Act, rights with regards to personal data are available to every data subject, wherever his nationality or residence.
<b>Third Party</b>	An individual who is not the subject of the data but may be connected to or affected by it is known as a third party.
<b>Relevant Professional</b>	The practitioners who supply information held on Social Services records, and various other medical and educational records. A relevant professional will consider where disclosure is likely to cause serious physical or mental harm to the applicant or any third party.

## Data Subject Rights

The right to access applies to all pupils, parents, staff and anyone else that we hold personal data about.

SARs cover all personal information held by the school regardless of the format it is in or where it is stored, whether it is closed, archived, and in some cases even deleted information (e.g. located in outlook deleted items). However, subject access goes further than this and an individual is entitled to be:

- Told whether any personal data is being processed;
- Given a description of the personal data and the reasons it is being processed;

Document name: SAR Policy & Procedure	Status: Draft	Page 2 of 8
Issue Date: June 2025	Review Date: Summer 2028	

- Informed of the recipients or categories of recipient to whom the personal data have been or will be disclosed;
- Given a copy of the personal data; and
- Given details of the source of the data (where this is available).

An individual can also request information about the reasoning behind any automated decisions taken about him or her, such as a computer-generated decision for benefit or a grant entitlement, or an assessment of performance at work.

The 'right to access' allows the requestor to receive information held about them, as a Data Subject. The requestor will not necessarily receive every version of information, if it is held in different ways or duplicated. Access is to the data, not the particular documents.

In some circumstances, for example with pupils, a parent or other person with authority may make the Subject Access Request on their behalf.

### **Roles and Responsibilities**

Adhering to the GDPR and Data Protection Act 2018 is the responsibility of every member of staff acting for or on behalf of the school. Subject access requests fall within the data protection statutory framework and the ability to identify and appropriately handle a request for information or to exercise any other rights is considered to be part of every employee's role.

<b>Head Teacher</b>	The Head Teacher holds overall responsibility for compliance with the Act.
<b>Business Manager/DPO</b>	The Business Manager acts as the Data Protection Officer for the school and has responsibility for the management of Subject Access Requests; this includes dealing with complaints from the Information Commissioners Office, general compliance issues and data subject queries and concerns. Ensures that SARs are responded to in a timely manner and that only data that the data subject is entitled to access are sent out. Also responsible for completing a double check of all SAR's before they are securely dispatched.
<b>Employees</b>	All employees, including temporary staff, must understand their duty of care to ensure the confidentiality of all personal data. In addition, they must have an understanding of this Policy and where to direct individuals enquiring about subject access requests.

### **How can an individual make a SAR?**

A valid SAR does not have to be made in writing, but it is good practice to have a written request or confirmation in writing, so that the scope of the request is clear.

No matter how a request is received there is no requirement for the requester to mention either the Data Protection Act or Subject Access for it to be a valid request. In some cases, the requester may even state the wrong legislation e.g. Freedom of Information Act, but the request will still be valid.

### **Requests for Information About Children**

Pupils attending any type of school have a right of access under the GDPR to their own information. They may exercise these rights on their own behalf if we believe they are competent to do so. Assessing competence is based on the age, maturity and level of understanding of the child. Each situation will be decided in collaboration with the professionals working with the child, but 12 years is regarded as a starting

Document name: SAR Policy & Procedure	Status: Draft	Page 3 of 8
Issue Date: June 2025	Review Date: Summer 2028	

point. A child should not be considered competent if it is evident that he or she is acting against their own best interests or under pressure from a parent or other person with authority.

When a child cannot act for themselves or the child gives permission, parents will be able to access this information on their behalf. At Pirton Hill Primary School, we consider that children of primary school age do not have sufficient maturity to understand their rights under Data Protection law and we therefore respond to SARs made by parents / person with parental responsibility (PR) on their behalf without seeking their consent.

Under the Education (Pupil Information) (England) Regulations 2005 (EPIR 2005) parents also have an independent right of access to their child's educational record, under separate education regulations. This covers information that comes from a teacher or other employee of a Local Authority or school, the pupil or a parent, and is processed by or for the School. It will cover information such as the records of the pupil's academic achievements as well as correspondence from teachers, Local Authority employees and educational psychologists engaged by the school's governing body. It may also include information from the child and from a parent. Information provided by the parent of another child would not form part of a child's educational record.

A request for an educational record must receive a response within 15 school days. The School can charge what it costs to supply a copy of the information. It is free for a parent to view the educational record.

There are certain circumstances where the school can withhold an educational record; for example, where the information might cause serious harm to the physical or mental health of the pupil or another individual. The request for access would also be denied if it would mean releasing examination marks before they are officially announced.

### **Requests Made on Behalf of Others**

The GDPR does not prevent an individual making a subject access request via a third party. Often, this will be a solicitor acting on behalf of a client. In these cases, checks should be carried out to satisfy that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority or might be a more general power of attorney.

When a SAR is received from a Law firm, the DPO must ensure that the request letter confirms that the School will not be a party to the claim. If the School is a party, legal advice must be sought. The request letter must also include a signed consent or release form from the client. The information disclosed should be exactly as outlined in the client's consent form. Information must not be released without the client's consent form.

The School must also be satisfied that the requester is entitled to the information. For example, a parent is not necessarily automatically entitled to all information about their children. The DPO will liaise with the Designated Safeguarding Officer to confirm the PR status of a parent.

### **How long do we have to respond?**

SARs must be responded to as soon as possible, and within one month at the latest. In the case of complex or multiple requests an extension of up to an extra two months can be applied. The requestor must be informed of the extension within the first month.

For SARs, the timescales for responding do not pause when the school is closed for holidays, bank holidays and weekends. For example, a valid SAR received on 20th July should be fulfilled by 20th August despite the school closure.

Document name: SAR Policy & Procedure	Status: Draft	Page 4 of 8
Issue Date: June 2025	Review Date: Summer 2028	

It is the responsibility of all staff to recognise a subject access request and process it accordingly. Failing to recognise a SAR is not an excuse for non-response and the School will still need to comply with the request in the statutory time period of a month (30 days) from receipt of the request.

### **Is there a charge?**

No fee can be charged for handling a request, however, a 'reasonable fee' can be charged when a request is:

- Manifestly unfounded or excessive, particularly if it is repetitive;
- For further copies of the same information.

The fee must be based on the administrative cost of providing the information.

### **What happens when SAR is received?**

All SARs must be directed to the DPO immediately.

In practice, if the request is simple e.g. someone wants to see a small part of their data (an exam result or written consent), we do not require a formal SAR if the individual can prove their identity, the information is readily available there and then, and no other third-party data will be unreasonably released. Such requests should be dealt with quickly and with little formality.

For requests which are likely to take a reasonable amount of resource, the DPO may ask the requester for further information or clarification that is reasonably required to find the personal data that they are seeking. The School is not required to comply with the request until this information is received, however there shouldn't be an unreasonable delay in seeking clarification.

Refer to Appendix 1 – SAR Procedure.

### **What information can and cannot be sent to the data subject?**

In limited circumstances, the request or elements of a SAR may be refused under the exemptions in the DPA 2018, for example:

- If the requestor cannot confirm their identity or authority to make the request on behalf of another person, the request will be refused until confirmation is provided;
- Where a request is manifestly unfounded or manifestly excessive;
- Information relating to education data, social work data or health data if it might cause serious harm to the physical or mental health of the data subject or another individual (this applies even when a competent child has consented to their parent receiving their data).
- Where legal professional privilege applies;
- Where management forecasts or negotiations could be prejudiced by disclosing the data;
- Confidential references; and
- Where exam results are requested but they are not yet due to be published.

There are restrictions where this would involve disclosing information about another individual (third parties). Where the person's data is combined with another person's data, which does or could identify the third party, that data may be redacted, or withheld if redaction would not fully prevent the other person being identified.

The third party's views on the release of this information to the applicant may be sought. Data can be disclosed that identifies the third party if that person has given their consent to disclose it. If, as a result of this consultation, information is to be edited it should be kept to a minimum and the context of information should always be retained where possible.

Document name: SAR Policy & Procedure	Status: Draft	Page 5 of 8
Issue Date: June 2025	Review Date: Summer 2028	

Decisions about disclosing third party information should be made on a case by case basis. It may be necessary to seek legal advice where appropriate.

Other elements of data that cannot be shared routinely without specialist consideration are:

- Information that would reveal that a child is at risk of abuse, where disclosure of that information would not be in the child's best interests (this applies even when a competent child has consented to their parent receiving their data);
- Safeguarding concerns which may contain information about multiple children including siblings and estranged parent;
- Information contained in adoption and parental order records;
- Certain information given to a court in proceedings concerning a child.

Where appropriate, the School will seek guidance from the Information Commissioner Office (ICO) and/or seek legal or professional advice to ensure compliance with the Act.

### **Record Keeping**

The receipt of SARs, all decisions made and the information provided will be stored in the School's Google Drive. This ensures timescales are being met and SARs are being handled appropriately.

The file will be retained for five years.

### **Complaints**

If an applicant is unhappy with the service, they have received or the response to their request they should contact the Headteacher.

As there is a statutory complaint process in place, these complaints will be dealt with outside the School's Complaint Policy. All complaints must be responded to within 1 month of receipt.

Where a complaint relates to the response to a subject access request, the response must include an explanation of why that response was not given.

If the applicant remains dissatisfied, they may ask the Information Commissioners Office to carry out an independent investigation.

Information Commissioner's Office  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire  
SK9 5AF

**Telephone:** 0303 123 1113

**Fax:** 01625 524510

<https://ico.org.uk/make-a-complaint/>

Document name: SAR Policy & Procedure	Status: Draft	Page 6 of 8
Issue Date: June 2025	Review Date: Summer 2028	

## **Appendix 1 – Subject Access Request Procedure**

This procedure supports our Data Protection Policy, and explains how we respond to requests from, or on behalf of, individuals for access to the data we hold that is about the individual. This is known as the right to access, and is a legal right under the UK GDPR and the DPA 2018. Requests are known as Subject Access Requests, or SARs.

In addition, parents have the right to access the child's curricular and educational records, under the Education (Pupil Information) (England) Regulations 2005 (EPIR 2005).

All staff are responsible for ensuring they read and understand this procedure as they may receive a SAR. Any individual who purposefully alters, defaces, blocks, erases, destroys or conceals information to prevent it being provided to a data subject who has requested it, and has a right to receive it, may be committing an offence.

### **Receiving a SAR**

A SAR does not need to be in writing, it can be in any format, including a letter, email, message via Weduc, over the telephone, or face to face, and can be made to any staff.

A SAR does not need to refer to data protection legislation or be described as a subject access request to be a valid SAR. Any request for access to personal information from, or on behalf of, a data subject, should be treated as a SAR.

Upon receipt of a SAR, the DPO must be informed without delay.

### **Checking the Identity and Authority**

The DPO must verify the identity of the person making the SAR, and if the SAR is being made on behalf of someone else, we must confirm they have authority to act on their behalf in exercising their rights.

Checking identity should not be used as a delaying tactic, and how to verify identity will depend on who is making the SAR, and how well they are known to the person handling the request. For example, a staff member will not usually be required to confirm their identity, but a request from a former staff member, or on behalf of someone else, may need to be verified.

At Pirton Hill Primary School, we consider that children of primary school age do not have sufficient maturity to understand their rights under Data Protection law and we therefore respond to SARs made by parents / persons with parental responsibility (PR) on their behalf without seeking their consent.

The DPO will liaise with the Designated Safeguarding Officer to confirm the PR status of a parent.

### **Responding to a SAR**

Once the identity and authority has been confirmed as valid, an acknowledgement should be sent to the requestor as soon as possible to inform them that the SAR has been received, the start date, and that it is being processed.

SARs must be responded to as soon as possible, and within one month at the latest. In the case of complex or multiple requests an extension of up to an extra two months can be applied. The requestor must be informed of the extension within the first month.

For SARs, school holidays, bank holidays and weekends are all included within the month. For example, a valid SAR received on 20th July should be fulfilled by 20th August despite the school closure.

Requests made under EPIR 2005 must be fulfilled within 15 school days.

Document name: SAR Policy & Procedure	Status: Draft	Page 7 of 8
Issue Date: June 2025	Review Date: Summer 2028	

The DPO will decide with the requestor, the most appropriate and preferred method of providing the requested information.

**What is a double check?**

Before a SAR is sent out to the data subject, SLT and the DPO are required to carry out a double check. This is done to ensure that all third-party data has been redacted and exempt data is not disclosed.

Third party data sent out in error to the wrong person constitutes a data breach under the Data Protection Act 2018 and can have very serious consequences for the School.

**Response**

When sending the relevant data to the requestor, the information should be clear, no any codes or jargon used should be explained in the SAR response and that they have the right to make a complaint to the ICO.

Regardless of the method of proving the information, the requester will be required to complete a 'Collection form' to confirm receipt of the information.

Document name: SAR Policy & Procedure	Status: Draft	Page 8 of 8
Issue Date: June 2025	Review Date: Summer 2028	