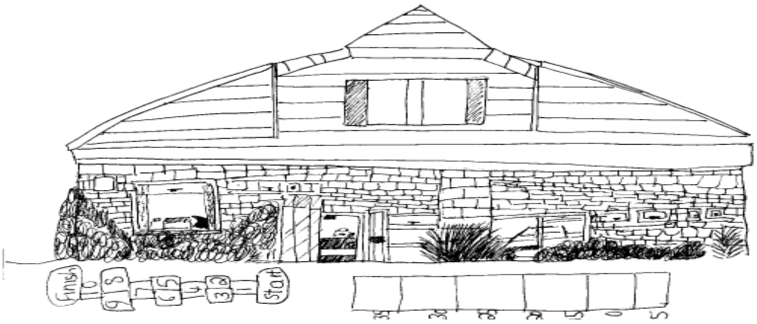
Graveley Primary School

A Church of England (VC) School



GDPR Subject Access Request Policy

Date policy updated	**Summer Term 2023**
Ratified by the Governing Board	**13/6/2023**
Date of next review	**Summer Term 2025 (or sooner if required)**

1. Introduction

1.1 The School holds personal data about many types of data subjects, such as employees, pupils, contacts and other individuals, for a variety of purposes, and is the data controller for such data.

1.2 Under the Data Protection Act (DPA 2018) and the UK General Data Protection Regulation (UK GDPR), individuals have the right to access and receive a copy of their personal data, and other supplementary information, held by us. This is commonly referred to as a subject access request or ‘SAR’.

2. Policy statement and objectives

2.1 The School is committed to the principles of lawfulness, accountability, transparency and the general right of access to information, subject to legal exemptions. We will make every effort to meet our obligations under the respective legislation, and this policy outlines how we manage our obligations for compliance.

2.2 This policy describes how an individual can make a request for their personal information and the processes that we will follow in order to comply with legal obligations for dealing with such requests.

2.3 All employees, including temporary staff, must understand their responsibilities under DPA 2018 and UK GDPR. In addition, they must have an understanding of this policy and the ability to identify and appropriately handle a request for information.

3. Key definitions

Subject Access Request (SAR)	A formal request from a data subject for information, including personal data, which an organisation holds about them.
Freedom of Information (FOI) Request	A request for access to data held by a public authority, which is not personal data, that is dealt with under the Freedom of Information Act (FOIA) 2000.
Personal data	Any information relating to an identified or identifiable natural person, and could be as simple as a name or a number, or could include other identifiers e.g. date of birth, photo, IP address, performance appraisal etc.
Special category data	Special category data is personal data that needs more protection because it is sensitive. The UK GDPR defines special category data as personal data revealing or concerning: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data (where used for identification purposes); health; and a person’s sex life or sexual orientation.
Data controller	Exercises overall control over the purposes and means of the processing of personal data. Controllers must comply with, and demonstrate compliance with, all the data protection principles as well as the other UK GDPR requirements.
Data processor	Acts on behalf of, and only on the instructions of, the relevant controller.

Data subject	Any living individual whose data is being held.
Data Protection Officer (DPO)	Monitors internal compliance, informs and advises on data protection obligations, and acts as a contact point for data subjects and the regulatory body.
Information Commissioner's Office (ICO)	Independent public body responsible for ensuring compliance with the UK's data protection regulations. Provides guidance, investigates breaches of the regulations and deals with complaints. The ICO has the power to impose monetary penalties or require specific actions to be taken to improve compliance in the event of a breach of the regulations.

4. Roles and responsibilities

4.1 Subject access requests fall within the data protection statutory framework, and the ability to identify and appropriately handle a request for information is considered to be part of every employee's role.

4.2 The primary responsibility of all staff is to understand how to recognise a request, and ensure that any such requests are sent to the Data Protection Officer. It is vital that requests are processed as soon as they are received in order to comply in meeting the statutory deadline.

Data Protection Officer	Elaine Dunnicliffe has overall responsibility for monitoring compliance
Data Protection Team	Nicky Hand and Nancy Yuen are responsible for assisting the DPO in ensuring that requests are responded to in a timely manner, that only information that the requester is entitled to access is disclosed, and for completing a thorough check of all requests before they are securely dispatched
All staff	All employees, including temporary staff, must understand their duty of care to ensure the confidentiality of all personal data, as well as an understanding of this policy and where to direct any requests

5. Receiving a subject access request

5.1 A data subject access request is a request from an individual or from someone acting on their behalf, e.g. a parent, for access to data that we hold about them.

5.2 A valid request will usually be made in writing by letter or email and even through electronic means such as social media. It can also be made verbally. There is no requirement for the requester to mention either the DPA 2018, UK GDPR or the term 'Subject Access Request' for it to be a valid request. In some cases, the requester may even cite the wrong legislation, but the request must still be responded to correctly.

5.3 The request for information can be very broad ("give me a copy of information you hold about me") or it can be very precise ("give me a copy of the letter you wrote about me yesterday").

5.4 Where a request has been made by another individual on behalf of the data subject, a number of checks and considerations will need to be made before processing the request (see **Actions on receipt of a request**).

5.5 A request is valid even if the individual has not sent it directly to the person who normally deals with such requests. It is important to ensure that all staff can recognise a SAR and treat it appropriately. Any member of staff receiving such a request must inform the DPO immediately.

6. Making a subject access request

6.1 A parent or guardian can request data in respect of their own child, where a child does not have sufficient maturity to understand their rights. Where we consider the student to be mature enough to exercise their own rights, [usually by the age of 13], their consent may also be required in the event of a request from a parent.

6.2 We would normally expect to respond to a request within one calendar month, however in the case of a more complex request, we may need to take up to an extra two months in order to fully respond.

6.3 In addition, we will alert requesters that as we have limited staff resources during school holiday periods, we would encourage requests to be submitted during term time, and not during periods when we are closed or are about to close for the holidays. This will assist us in responding to any request as promptly as possible. If requests are received when we are closed, it is very likely that we will need to extend our response time.

6.4 Requests for information should be sent to our DPO – Elaine Dunnicliffe (elaine.dunnicliffe@graveley.herts.sch.uk)

6.5 Although it is not compulsory, the School would encourage anyone making a request to use the form (on p11 of this policy). This will help them to structure their request and prompt them to include the necessary details to enable us to locate more precisely the data that is needed.

6.6 As a minimum, the following information should be supplied, as laid out in the guidance supplied by the ICO on their website.

- the requester's name plus any other information to identify or distinguish them from other individuals;
- the requester's up-to-date contact details;
- if they are not the data subject, then their relationship to them, along with full details of the data subject, and their consent (if required);
- a comprehensive list of what personal data the requester wants to access, based on what they need;
- any details, relevant dates, or search criteria that will help us identify what they want; and
- how they would like to receive the information (i.e. electronically or as hard copy).

6.7 If they do not supply this information, then it could take us longer to respond to their request, and may also make it more difficult for us to locate the specific information that they are looking for. Where we have asked for further clarification, and we process a large amount of information about the data subject, then it is likely that the time limit for responding to the request will be paused until we receive their response.

6.8 Where the identity of the requester is in doubt, we will need to ask for supporting evidence to verify their identity, including where necessary their relationship to the data subject, and in those circumstances the time limit for responding will be paused until this has been received and checked. Such proof may include a passport, driving licence, recent utility bill with current address, birth/marriage certificate, credit card, mortgage statement or court orders.

6.9 There are certain circumstances where we may refuse to disclose part of the data, where disclosure of the information might cause serious harm to the physical or mental health of the pupil or another individual.

6.10 The Education (Pupil Information) (England) Regulations 2005 give parents of children who attend maintained schools a right to access their child's educational records. This is a separate statutory right that parents have aside from the DPA 2018, subject to any court orders which may be in place. The educational record covers the majority of information that is processed by us, except for certain information e.g. that which teacher has solely for their own use, or information provided by the parent of another child. A request for an educational record must be responded to within 15 school days. We can charge what it costs to supply a copy of the information, but it can be viewed free of charge. Such requests are not regulated by the ICO and are outside of the scope of the DPA 2018 and UK GDPR. Further details for accessing information about pupils can be found on the ICO's website.

7. Actions on receipt of a request

7.1 We must comply with a SAR without undue delay and usually within one month of receipt of the request. Where we have asked for further information, either to confirm the requester's identity or to clarify the scope of the data required (where large volumes of data are involved), we can pause the time limit for responding until we have received that information.

7.2 However, in the case of a more complex request, we can take up to an extra two months in order to fully respond. This will be determined on a case by case basis, and will be communicated to the requester within the first month. We will aim to supply as much information as we reasonably can by the end of the first month, and after that will continue to keep the requester informed regarding progress.

7.3 When receiving a SAR, the first steps we will take are as follows:

7.3.1 We will ascertain whether the request is a formal SAR. If someone only wants to see a small part of the data e.g. assessment or exams data, then it may not require a full response in the form of a SAR. Such requests should be dealt with quickly as 'business as usual'.

7.3.2 We will acknowledge the request as soon as possible, and where necessary will ask for proof of identity. We will only ask for this where we do not have an ongoing relationship with the requester or where their details are not already known to us. Proof of identity may require production of a passport, driving licence, recent utility bill with current address, birth/marriage certificate, credit card, mortgage statement or court orders. Where this information is not provided immediately, we can pause the timescale for responding to the request until it is received.

7.3.3 If the request was initially made verbally, we will always ask for confirmation in writing to follow. In the case of a parent making a request for the personal data of a child [aged 13 or over], we may also need to request confirmation that they consent to disclosure.

7.3.4 If it is not clear what data is being asked for or the request is very broad, we will ask the requester to provide additional details, including relevant dates or search criteria that will help us to identify the required data, and advise them that we may need to pause the time limit for responding to the request until this information has been received. However, if the individual refuses to provide any additional information, we must still comply with their request by making reasonable searches for the information.

7.3.5 If any further information that we have requested is not received, or the requester makes no further contact, we will wait for one month before considering the request as 'closed'.

7.3.6 Once the validity and scope of the request has been confirmed, we will send further correspondence to confirm this with the requester, along with the proposed timescale for the response.

7.3.7 If the request is complex, we can extend the time to respond by up to a further two months from the original start date, providing that we are able to justify this, and must inform the requester within one month of receiving their request. Where it is appropriate, we will explain why further time is necessary. The following reasons may apply:

- technical difficulties in retrieving the information, e.g. if data is electronically archived
- applying an exemption that involves large volumes of particularly sensitive information
- clarifying potential confidentiality issues around the disclosure of sensitive medical information to an authorised third party
- clarifying potential issues around disclosing information about a child to a legal guardian
- any specialist work involved in obtaining the information or communicating it in an intelligible form
- needing to obtain specialist legal advice
- searching large volumes of unstructured manual records

7.4 An entry will be made in our subject access log, showing: the date of receipt; the data subject's name; the name and address of requester (if different); consent given (if necessary); details of the type of data required, and search terms to be used; how the information will be supplied; and the planned date for supplying the information.

8. What information needs to be provided as part of a request

8.1 As well as a copy of the personal data we hold as defined in the scope of the request, individuals have the right to receive the following supplementary information:

- our purposes for processing;
- categories of personal data we are processing;
- recipients or categories of recipient we have or will be disclosing the personal data to;
- our retention period for storing the personal data or the criteria for determining how long we will store it;
- the individual's right to request rectification, erasure or restriction or to object to processing under certain circumstances;
- the individual's right to lodge a complaint with the ICO;
- information about the source of the data, if it was not obtained directly from the individual;

- whether we use automated decision-making (including profiling) and information about the logic involved, as well as the significance and envisaged consequences of the processing for the individual; and
- the safeguards we have provided where personal data has or will be transferred to a third country or international organisation.

8.2 As most of the above are addressed in our privacy notices, we will supply a copy of the relevant privacy notice, or a link to its location on our website, to the requester. Any relevant supplementary information not in the privacy notice will be added to the covering letter sent with the personal data.

9. Locating the information to be provided

9.1 The UK GDPR places a high expectation on us to provide information in response to a SAR. Therefore we will make reasonable efforts to find and retrieve the requested information. However, we are not required to conduct searches that would be unreasonable or disproportionate to the importance of providing access to the information.

9.2 To determine whether searches may be unreasonable or disproportionate, we must consider:

- the circumstances of the request;
- any difficulties involved in finding the information; and
- the fundamental nature of the right of access.

9.3 The personal data that we need to provide may be located in a number of electronic and manual filing systems. Depending on the type of information requested, we may need to search all or some of the following:

- electronic systems e.g. our Management Information Systems (MIS) which is Arbor, other databases, networked and non-networked computers, servers, email data, back up data.
- manual filing systems in which personal data is accessible according to specific criteria, e.g. manual records containing personal data sorted alphabetically or chronologically;
- data systems held externally by our data processors;
- personnel records;
- occupational health records held by our OH provider
- pensions data;

9.4 We will carry out reasonable and proportionate searches, using the appropriate search criteria for the type and location of the personal data e.g. name, UPN, employee number or other personal identifier. We may also need to speak to members of staff who might hold information about the individual.

9.5 Once we have collected together the information held about the individual, we will examine it in detail to establish if it can be released. This will be done on a case-by-case basis for each individual piece of information. In some cases, we might have to disclose only parts of particular documents. In addition, we must:

9.5.1 Check that the information is actually about the person concerned and not someone else with the same name;

9.5.2 Screen out any duplicate records.

10. Exemptions

10.1 The DPA 2018 defines a number of circumstances where an exemption might apply, in particular regarding disclosure of information which identifies another individual. We will only disclose information relating to a third party where it is appropriate to do so. This decision will be made on a case by case basis, and involves balancing the data subject's right of access against the other individual's rights relating to their own personal data. We may decide to disclose such data where:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

10.2 As our obligation is to provide information rather than documents, we may delete names or edit documents if the third party information does not form part of the requested information. Therefore we may provide the information in the form of transcripts of relevant documents, or of sections of documents that contain the personal data, or by providing a print-out of the relevant information from our systems. We must take into account all the relevant circumstances, including:

- the type of information to be disclosed;
- any duty of confidentiality owed to the third party;
- any steps taken to try to get the third party's consent;
- whether the third-party individual is capable of giving consent; and
- any stated refusal of consent by the third-party individual.

10.3 Where we have made a decision not to disclose certain information, we will explain why, **except** if the reason relates to safeguarding/child protection concerns.

10.4 Examples of third party information that cannot be shared routinely without special consideration include, but are not limited to:

- Safeguarding or child protection data;
- Files containing legally privileged information;
- Files containing advice from relevant professionals such as doctors, police or probation services; and
- Employee files containing information identifying other colleagues who have contributed to (or are discussed in) the file.

10.5 We must be able to justify our decision to disclose or withhold information about a third party, so we will keep a record of any exemptions applied, and the reasoning behind these, to ensure that there is an audit trail in the event that this is queried by the requester or the ICO.

11. Refusing to respond to a request

11.1 We can refuse to comply with a SAR if it is manifestly unfounded or manifestly excessive. However, we would require strong justifications for this, which we could clearly demonstrate to both the individual and the ICO.

11.2 A request may be manifestly unfounded if the individual clearly has no intention to exercise their right of access or the request is malicious in intent. A request may be considered manifestly excessive if it is clearly or obviously unreasonable. However, a request is not necessarily excessive just because a large amount of information has been requested.

11.3 We must consider each request in the context in which it is made. If a request is found to be manifestly unfounded or excessive then we may decide to request a 'reasonable fee' to deal with the request, or refuse to deal with the request.

12. Providing the information

12.1 The information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Therefore the information should: not include information that is irrelevant or unnecessary; be open, honest and truthful; be easy to understand by the average person (or child); be easy to access; and use common, everyday language.

12.2 The information will be provided either in the form of Portable Document Format (PDF) files and/or as hard copy documents, depending upon how the requester submitted their request or gave their preference.

12.3 We will add a label to the information provided to the requester with 'requester's copy'. This may help identify the source of any further disclosure of the information, should the need arise.

12.4 Although we cannot require the requester to take actions in order to receive the information, we may ask them to collect large volumes of hard copy data from us and sign to acknowledge receipt. However, if they do not agree to this we will send the documents securely. Depending on the nature and sensitivity of the information, we may need to consider sending it by special delivery or via a courier service.

12.5 If we are providing the information electronically, we will use an appropriately secure method, which may be to encrypt and password protect the files, followed by sending the password to the individual separately or by using a secure file transfer system such as Schoolsfx [or other secure method e.g. secure link].

13. Requests from the Police or other Agencies

13.1 When a request for personal data is made in relation to the prevention and detection of a crime, the prosecution of offenders, or to protect the vital interests of a person, then an exemption rule can be used to disclose personal data without breaching the DPA 2018 or UK GDPR.

13.2 The request should explicitly state a specific reason for providing the data and must come from a verified source. As the data controller, we must then make a decision as to whether the request is reasonable, and whether to share the data.

13.3 Any request for information from an outside agency, including the police or local authority, should be made officially in writing and preferably using a standard form. However, where there is an urgent need and time is of the essence, we may consider a verbal request as long as it is followed by a written request. This is necessary to provide a clear audit trail that we can use to demonstrate our decision to share the information.

14. Complaints Procedures

14.1 We provide a right of complaint to all requesters in the event they are dissatisfied with the handling of their request. The ICO provides guidance on how to complain on their website. Any such complaints should be directed to our DPO at elaine.dunnicliffe@graveley.herts.sch.uk who will make an independent assessment of the case.

14.2 If the requester remains dissatisfied then they can contact the ICO either via their helpline number 0303 123 1113 or via their website.

15. Policy Review

15.1 This policy is reviewed every 2 years with reference to the relevant legislation or guidance in effect at the time. Further reviews will take place as required.

Appendix 1 – Subject Access Request Form

SUBJECT ACCESS REQUEST FORM

Section 1: Details of data subject

If you are not the data subject, and you are requesting the data on behalf of someone else e.g. your child, please fill in their details in Section 1 and your own details in Section 2.

Relationship with school:	Pupil / parent / employee / governor / volunteer / other (please specify)
Title:	
Surname:	
First name(s):	
Date of birth:	
Sex:	
Address:	
Phone number:	
Email address:	

Personal Information required In order for us to respond to your request in the shortest possible timeframe, please can you provide us with some additional details to help us locate the requested information, including a comprehensive list of what personal data you want to access plus any specific details, relevant dates, or search criteria that will help us to identify and find what you want. *For more information please see the ICO's guide to submitting a request here:* https://ico.org.uk/your-data-matters/your-right-to-get-copies-of-your-data/preparing-and-submitting-your-subject-access-request/

Section 2: Details of data requester

Please complete this section of the form with your details if you are acting on behalf of someone else.

Title:	
Surname:	
First name(s):	
Sex:	
Address:	
Phone number:	
Email address:	

Relationship to data subject	Parent / Carer / Legal Representative / Other (please specify)

Proof of identity

We may need to ask you for proof of identity, and where applicable, proof of authorisation to act on behalf of the data subject. If this is the case, we will contact you with a list of what you will need to provide.

How to receive the information

I wish to receive the information:

□ By post*

□ By email/secure file transfer

□ By collection in person

*Please be aware that if you wish us to post the information to you, we will take every care to ensure that it is addressed correctly. However, we cannot be held liable if the information is lost in the post or incorrectly delivered or opened by someone else in your household.

Please send this completed form to: elaine.dunnicliffe@graveley.herts.sch.uk

Document Control

Date modified	Description of modification	Modified by