SUTTON VALENCE SCHOOL
SINCE 1576

Subject Access Rights Policy and Procedure

(Prep School and Senior School)

Author: Mr Glen Millbery
Policy Date: September 2025
Approval Date by Governors: November 2025
Review Date: September 2026

This Policy applies to Sutton Valence School (including as the context requires, the Nursery, the Prep School and the Senior School).

Data Subject Access Request Policy and Procedure

1. Purpose

1.1. This policy and procedure establishes an effective, accountable and transparent framework for ensuring compliance for data subject access requests according to the GDPR regulations.

2. Policy Statement

2.1. The GDPR details rights of access to both manual data (which is recorded in a relevant filing system) and electronic data for the data subject. This is known as a Data Subject Access Request (DSAR).

2.2. Under the GDPR, Sutton Valence School is required to respond to subject access requests within one month. Failure to do so is a breach of the GDPR and could lead to a complaint being made to the Data Protection Regulator.

2.3. This policy informs staff of the process for supplying individuals with the right of access to personal data and the right of access to staff information under the General Data Protection Regulation (hereinafter called GDPR).

3. Procedure

How DSARs should be processed after receiving

3.1. When a subject access request is received from a data subject, it should immediately be reported to the DCO who will log and track each request. If we are asked to provide information, the following must be considered before deciding how to respond:

- Under GDPR Articles 7(3), 12, 13, 15-22 data subjects have the following rights:
  - to be informed;
  - to access their own data;
  - to rectification;
  - to erasure (Right to be Forgotten);
  - to restriction of processing;

- to be notified;
- to data portability;
- to object;
- to object to automated decision making.

- Requests can be made in any format and to any member of staff.
- The type of access we must provide and the fee we are allowed to charge may vary depending on how the records are held. It does not have to state 'subject access request' or 'data protection' to constitute a request under the GDPR.
- If a request has already been complied with and an identical or similar request is received from the same individual, a fee can be charged for the second request unless a reasonable interval has elapsed.
- The statutory response time is one month.
- Requests should include the full name, date of birth and address of the person seeking access to their information. To comply with the GDPR, information relating to the individual must only be disclosed to them or someone with their written consent to receive it.
- Before processing a request, the requestor's identity must be verified. Examples of suitable documentation include:
  - Valid passport;
  - Valid identity card;
  - Valid driving licence;
  - Birth certificate, along with some other proof of address e.g. a named utility bill (no longer than three months old)

3.2. If there is information that relates to third parties, we will write to them asking whether there is any reason why this information should not be disclosed. We do not have to supply the information to the individual making the DSAR unless the other party has provided their consent or it is reasonable to do so without their consent.

3.3. Before sharing any information that relates to third parties, we will, where possible, anonymise information that identifies third parties where consent has not been given. We may also summarise information rather than provide a copy of the whole document. The GDPR requires us to provide information not documents.

3.4. The DSAR will take the following steps:

1. Discovery;
2. Sifting;
3. Exemption;
4. Redaction;
5. Checking.

- Discovery – this is where we pull all the possibly relevant information – this is mostly done electronically and pools it in a single location. This will include irrelevant information;
- Sifting – this is where a human needs to go through every piece of information found and determine if it is relevant to the subject access request;
- Exemption – this is where every piece of information that is relevant is looked at to determine if it is to be handed over or if there is some reason (an exemption) why it should not be. If there is an exemption suggested, then a suitably qualified third party,

unrelated to those involved in the DSAR will look over the material and confirm / deny the exemption.

- Redaction – this is where any personal details relating to individuals other than the person requesting the subject access request are removed;
- Checking – this will be done by a member of staff who is not connected to the DSAR and will verify that the information collated relates to the purpose, does not violate anyone else's privacy and that all exemptions have been acted upon.

4. GDPR Sentry

4.1. GDPR Sentry will be used to log the SAR and its progress.

5. Fees

5.1. No fee can be charged for providing information in response to a data subject access request, unless the request is 'manifestly unfounded or excessive', in particular because it is repetitive. If Sutton Valence School receives a request that is manifestly unfounded or excessive, it will charge a reasonable fee, taking into account the administrative costs of responding to the request. Alternatively, Sutton Valence School will be able to refuse to act on the request.

6. Subject Access Requests made by a Representative or Third Party

6.1. Anyone with full mental capacity can authorise a representative/third party to help them make a data subject access request. Before disclosing any information, Sutton Valence School must be satisfied that the third party has the authority to make the request on behalf of the requestor and that the appropriate authorisation to act on their behalf is included.

7. Complaints

7.1. If an individual is dissatisfied with the way Sutton Valence School have dealt with their subject access request, they should be advised to invoke the complaints process. If they are still dissatisfied, they can complain to the Data Protection Regulator.