GSA Students' Association

Subject Access Request Protocol

This protocol is for use by any member of staff who receives a subject access request for GSASA.

The Data Protection Officer for GSASA is the Acting General Manager, Lauren Macfadyen.

What is a Subject Access Request?

A SAR is a request from an individual, or by an authorized agent/parent/guardian of that person, for a copy of their personal data being held by GSASA and information about that data.

- It does not have to be in any particular form, as long as it's clear that the individual is asking for their own personal data.
- It can be a written or verbal request.
- It can also be submitted by email or social media.
- Requests do not need to contain the words "subject access request" or reference "Article 15 of the GDPR" to be valid.
- A SAR can be made to any member of staff.

What information is an individual entitled to?

Individuals have the right under the Data Protection Act 2018 (DPA) and the EU General Data Protection Regulation (GDPR) to find out what information is held about them and why it's held by us.

- Confirmation that you are processing their personal data
- The purposes of your processing;
- The categories of personal data concerned
- The recipients or categories of recipient you disclose the personal data to;
- Your retention period for storing the personal data or, where this is not possible, your criteria for determining how long you will store it;
- The existence of their 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;
- Information about the source of data; where it was not obtained directly from the individual

Much of this information is available in the GSASA Privacy Notice and data retention schedule.

The requester is entitled to see their own personal data only.

There are some exceptions to this entitlement, see **Annexe 2**.

The requester is entitled to see this data in an easily accessible form, using clear and plain language, with any jargon or codes explained.

What is the time limit for responding?

In most cases you must respond to a subject access request promptly and within **1 calendar month** of GSASA receiving it.

It is acceptable to wait to start the clock until receiving from the requester proof of their identity (see Step 2 below) and any additional information you require to process their request (see Step 3 below) so long as you do not delay with this process. [1]

Is there a fee to submit a SAR?

No. From the GDPR states Subject Access Requests must be free of charge. The only exception is if the request is 'manifestly unfounded or excessive', where an organisation is entitled to charge a 'reasonable fee'. It is also possible to charge a 'reasonable fee' if an individual requests further copies of their data.

Where requests are manifestly unfounded or excessive, you also can refuse to respond. If you do this, you must explain why to the individual, and inform them of their right to complain to the supervisory authority (The ICO).

Some definitions

Data Subject

The Data Subject is the individual about whom data is being kept. For us, this might be a student, member of staff, supplier, etc. This is usually also the person who submits the subject access request; however, it is possible that the Data Subject will ask a third-party, such as a solicitor, to make the request on their behalf.

Personal data

Personal data is any information held on a living individual which will allow that individual to be identified. Data items that allow identification include: name, address, date of birth, National Insurance number, etc. It includes all information which is obviously about the Data Subject or their activities, or has some biographical connection to them.

Personal data covers both facts and expressed opinions about the individual.

[1] ICO SAR Code of Practice states that "you should not delay" in asking the requester for more information and should "ensure that the requester knows you need more information and should tell them what details you need." Providing you have done this, "the period for responding to the request does not begin to run" until you have received the information you need to process the request. (2017: p29)

Personal data can take the form of text and images (photos and videos). It can be held on a computer, on paper or on electronic media. Email correspondence which involves or mentions the Data Subject is considered personal data.

Procedure for dealing with Subject Access Requests

When a Subject Access Request is received by any member of GSASA staff, the following procedure should be followed.

If the request is a normal part of the day-to-day business of the department, it should simply be treated as day-to-day business. For example, if a member of staff asks for their payroll number this should be answered as a normal business query. There is no need to follow the formal procedure below.

However, if a request goes beyond the normal business transactions of a department, it must be dealt with formally according to the following procedure.

1. Inform the Data Protection Officer

As soon as you receive a Subject Access Request, inform the Data Protection Officer.

The Data Protection Officer will be able to provide you with guidance on how to respond to the request.

2. Confirm the identity of the Requester

It is very important to confirm the identity of the Requester to avoid the damage of inadvertently disclosing personal information to the wrong person. The Data Protection Officer will ask for any evidence GSASA requires to confirm the Requester's identity. In the case of requests made by a Third Party, the Data Protection Officer will ask for proof of relationship/authority.

3. Establish whether more information is needed to respond to the request.

If the Requester has not been clear about exactly what information they want to see, the Data Protection Officer will contact them promptly for any other information that is needed to respond to the request.

It might involve the requester sharing the identities of people or departments whom they expect to hold relevant information. If the requester wants to see CCTV images of them, for example, this might mean asking for a photograph of them, description of clothes worn, dates of visits, etc.

4. Contact the relevant areas and staff within GSASA

Once the scope of the request has been ascertained from the Requester, the Data Protection Officer will contact each relevant area to request that they gather the information required.

Each area should gather the request as follows.

5.Collate the information

The manager(s) of each area are responsible for ensuring that the information required from the SAR is collated.

6. Changing information after the request has been received

It is permissible to make routine amendments and deletions to personal data after the request has been received, but only if these would normally happen.

You are not permitted to make changes to the data as a result of receiving the request.

7. Remove information about other people

If the data includes information about other people, you must not supply it to the requester unless the other people mentioned have given consent for the disclosure.

You must still disclose as much information as possible by redacting the references to other people.

The data must be edited to remove references to others. See ANNEX 1 for guidance on redaction.

If it is not possible to separate or redact the personal data of a third party from the personal data of the requester, you do not have the third party's consent for disclosure, *and* you are not satisfied that it would be reasonable to disclose that information without consent, that particular information may be exempt from disclosure in the SAR.

8. Remove any information which is exempt

Certain types of information, such as confidential references, are exempt from disclosure by Subject Access Request. See ANNEX 2 for information about exemptions.

9. Explain any complex terms or codes

If the data includes any complex terms or codes, you must make sure that these are explained so the data can be understood.

10. Prepare the Response

Areas must provide two copies of the information in a permanent form. This can be in an electronic or printed form, whichever the Requester prefers. One copy will be retained by GSASA as a record of the response; the other copy will be sent to the requester.

In cases where the material is to be supplied from a number of different areas of GSASA the material should be collated in full by each area first. The response and accompanying checklist should then be sent to the Data Protection Officer for final collation.

11. Keep a record of the Response

GSASA will retain the record of the response. This may be referred to if there is any dispute. Such records should be retained for six months, and destroyed promptly thereafter.

You should remind anyone who makes a SAR of these rights:

- The right to lodge a complaint to the ICO.
- The right to request rectification, erasure or restriction of the relevant data.

12. Dispatch the Response

Send the response to the requester, and ask for confirmation of receipt. If the data is collated from multiple areas of GSASA, the response will be sent by the Data Protection Officer. If the data is held by a single area then that area should send the response, and the Data Protection Officer must be notified so the response can be recorded.

Where there is a large amount of material, it might be appropriate to arrange for collection by the requester. If third-party is uplifting the response on behalf of the requester, their identity and authorisation to act on the behalf of the requester must be confirmed.

ANNEX 1: GUIDANCE FOR STAFF UNDERTAKING A SEARCH FOR PERSONAL INFORMATION IN RESPONSE TO A SUBJECT ACCESS REQUEST

Staff may be required to search their files, including emails and paper files, for “Personal data” pertinent to a Subject Access Request.

Regarding the scope of the search:

1. The search should only include materials pertinent to the request. This might be very specific or very general depending on the detail of the request.
2. The search will normally only cover systems owned by GSASA. However if there are reasonable grounds to assume that relevant data might be held on personal devices which are not owned by GSASA, but which are used by GSASA staff for work, (phones, personal laptops, etc.) then these should also be included in the search.

Once such documents have been identified consideration must be given to whether there is any data relating to third parties also contained within them, which must not be divulged.

1. Where there is no information relating to third parties, no redaction (i.e. ‘blanking out’) is required and the document should be printed as it is.

2. There will be some documents which contain data relating to third parties, but which the Data Subject was already privy to (because, for example, the document is one that was created or seen by them in the ordinary course of his work). In these circumstances no redaction is required and the document should be printed as it is.

In all other cases where there is data relating to third parties, you must supply only the personal data relating to the Data Subject along with the context of the document. This can be done in two ways:

- by copying and pasting only the section relevant to the Subject, along with the title and date of the original, into another document to be printed out; or
- by blanking out (redacting) the information relating to third-parties so that it cannot be read.

ANNEX 2: DATA WHICH IS EXEMPT FROM DISCLOSURE

There are several classes of information which are exempt from disclosure under the Data Protection Act.

Some important examples include:

- Protecting the privacy rights of others: The DPA 2018 says that you do not have to comply with the request if it would mean disclosing information about another individual who can be identified from that information, except if the other individual has consented to the disclosure; or it is reasonable to comply with the request without that individual's consent.
- Confidential references: References about an individual, which you have given to or received from a third party, are exempt from subject access if you give them in confidence and for the purposes of an individual's education, training, volunteering or employment or the provision of a service by them.
- Management forecasts: Personal data that is processed for management forecasting or management planning (such as planning redundancies) is exempt from the right of subject access to the extent that complying with a SAR would be likely to prejudice the business or other activity of the organisation.
- Negotiations: Personal data that consists of a record of GSASA's intentions in negotiations with an individual is exempt from the right of subject access to the extent that complying with a SAR would be likely to prejudice the negotiations.
- Legal privilege: Information that comprises confidential communications between GSASA and a professional legal adviser may be withheld under the legal privilege exemption.