Data Protection

Subject Access Request Protocol

Policy control

<table>
<thead>
<tr>
<th>Reference</th>
<th>Subject Access Request Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date approved</td>
<td>5&lt;sup&gt;th&lt;/sup&gt; May 2015</td>
</tr>
<tr>
<td>Approving Bodies</td>
<td>Executive Group</td>
</tr>
<tr>
<td>Implementation Date</td>
<td>5&lt;sup&gt;th&lt;/sup&gt; May 2015</td>
</tr>
<tr>
<td>Supporting policy</td>
<td>Data Protection Policy</td>
</tr>
<tr>
<td>Review date</td>
<td>December 2017</td>
</tr>
<tr>
<td>Author</td>
<td>Colin Watson</td>
</tr>
</tbody>
</table>
Subject Access Request Protocol for Glasgow School of Art

Scope

Who should use this protocol?
This protocol should be used by any member of staff who receives a request from an individual asking for a copy of any personal data which is held by GSA (i.e. a Subject Access Request).

Background

What is a Subject Access Request?
A Subject Access Request (SAR) is a written request made by or on behalf of an individual for information about them which GSA holds on record. He or she is entitled to ask for this personal information under the Data Protection Act 1998 (DPA). The request does not have to be in any particular form. Nor does it have to include the words ‘subject access’ or make any reference to the DPA. However the request must be submitted in writing.

What information is an individual entitled to?
Subject access is most often used by individuals who want to see a copy of the information an organisation holds about them.

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, the reasons it is being processed, and whether it will be given to any other organisations or people;
- given a copy of the personal data; and
- given details of the source of the data (where this is available).

Often the easiest way to provide the relevant information is to supply copies of original documents, but you are not obliged supply complete documents. Subject access provides a right for the requester to see their own personal data only.

What is the time limit for responding?
In most cases you must respond to a subject access request promptly and in any event within 40 calendar days of GSA receiving it.

Definitions

Data Subject
The Data Subject is the individual about whom data is being kept. e.g. a student, member of staff, supplier, etc. This is usually also the person who submits the subject access request; however it is
Subject Access Request Protocol

possible that the Data Subject will engage 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.

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 GSA 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.

Notification of the Receipt of Request

1. Inform GSA’s Data Protection Officer
Any member of staff receiving a Subject Access Request must inform GSA’s Data Protection Officer immediately via email:

GSA’s Data Protection Officer is currently Colin Watson, the Head of IT (c.watson@gsa.ac.uk).

The Data Protection Officer will be able to provide you with guidance regarding the appropriate response to the request. If necessary the Data Protection Officer will be able to call upon legal advice to inform GSA’s response.

Validate and Substantiate the Request

2. Confirm the Identity of the Requester
The Data Protection Officer will ask the requester for any evidence GSA reasonably needs to confirm their identity. If the requester is acting on behalf of another person, GSA will ask for evidence that they have authorisation from the Data Subject to act on their behalf.
3. Promptly ask the Requester to pay the £10 admin fee
GSA charges a £10 administration fee for processing any Subject Access Request. The Data Protection Officer will ask the individual promptly to pay the fee. The 40 calendar day time limit starts when the fee has been received.

4. Establish whether more information is needed to clarify the request
Has the requester been clear about exactly what information they wish to see? If not, the Data Protection Officer will contact them promptly for the other information that GSA reasonably needs to find the information they want. For example, this might involve them clarifying the identities of people or departments whom they expect to hold relevant information.

5. Identify the Responsible Departments
Any general SAR can involve an extended search by many departments. Consequently, when you receive a request, and it is apparent that the information is held by more than one department, the Data Protection officer must be informed.

The Data Protection Officer will consult with departments and individuals within GSA to establish where the data is held, and establish who will be involved in the search.

Once the extent of the search has been determined the Data Protection Officer will convey this, via the Director of IT, to the Registrar (or other member of the Executive if the Registrar is not available) who will issue the instruction to all relevant departments to undertake the search for information.

The departments who hold the data are responsible for processing their part of the request as follows.

Processing the Request

6. Collate the information
If GSA holds relevant information, the department (or departments) that hold the information must gather the information requested.

See ANNEX 1 for Guidance to be followed by any staff who are required to conduct a search of their files for personal information relating to a Subject Access Request.

Members of GSA’s Executive Group have overall responsibility for ensuring that the information in their management area is collated.

Heads of School/Department (academic and service) have responsibility for ensuring that the information in their respective areas is collated.

See ANNEX 3 for a checklist to be completed by the responsible Head of School/Department before returning the data to the Data Protection Officer.

If GSA does not hold the information that the requester wants, the Data Protection Officer will inform them at this stage, and this null response will be recorded.
7. 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.**

8. 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. i.e. the data must be edited to remove references to others. See ANNEX 1 for guidance on redaction.

9. Remove any information which is exempt
Certain types of information, such as examination scripts and confidential references, are exempt from disclosure by Subject Access Request. See ANNEX 2 for information about exemptions.

10. 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.

For example if your data includes course codes, these should be explained giving the full title of the course.

11. Prepare the Response
Departments must provide two copies of the information in a permanent form. This usually means a printed copy, unless the individual agrees otherwise, or doing so would be impossible or involve disproportionate effort. One copy will be retained by the Data Protection Officer 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 departments or areas of GSA, the material should be collated in full by each Department/School first. The checklist in ANNEX 3 must be completed, signed and included with each departmental response. The response and accompanying checklist must then be sent to the Data Protection Officer for final collation.

12. Keep a record of the Response
The Data Protection Officer 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.

13. Dispatch the Response
Send the response to the requester, and ask for confirmation of receipt. If the data is collated from multiple departments, the response will be sent by the Data Protection Officer. If the data is held by a single department then that department 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. The relevant information should be printed out in hardcopy where possible. (If the result of the search produces a very large amount of data, other methods of disclosure may be considered, but hardcopy is preferred.)

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 GSA. However if there are reasonable grounds to assume that relevant data might be held on personal devices which are not owned by GSA, but which are used by GSA 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. GSA’s Data protection Officer can advise on this, but some important examples include:

- Examination scripts. Information comprising the answers given by a candidate during an examination is exempt from the right of subject access. So a SAR cannot be used to obtain a copy of an individual’s examination script. (However this exemption does not extend to an examiner’s comments on a candidate’s performance in an examination, or details of marks awarded. There are special rules governing this.)

- References about an individual, which you have given to a third party, are exempt from subject access if you give them in confidence and for the purposes of an individual’s education, training or employment or the provision of a service by them. There is no such exemption for references you receive from a third party.

- 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.

- Personal data that consists of a record of GSA’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.

- Information that comprises confidential communications between GSA and a professional legal adviser may be withheld under the legal privilege exemption.
ANNEX 3

CHECKLIST TO BE COMPLETED BY HoD/HoS WHEN DATA IS COLLATED

This checklist must be completed, signed, and attached to the response submitted by each Department.

Academic Departments should return the completed response to their Head of School along with this checklist confirming that the response is complete. The Head of School will then collate all responses from their departments, and return the combined response to GSA’s Data Protection Officer along with all checklists confirming that the response is complete.

Non-academic Departments should pass the completed response directly to GSA’s Data Protection Officer along with this checklist confirming that the response is complete.

Completed by Department: _________________________________

Relating to the following Subject Access Request: ____________________________________

<table>
<thead>
<tr>
<th>ACTION</th>
<th>TICK</th>
</tr>
</thead>
<tbody>
<tr>
<td>All relevant individuals have been consulted</td>
<td></td>
</tr>
<tr>
<td>All relevant data is included in the enclosed response</td>
<td></td>
</tr>
<tr>
<td>No relevant data has been changed except for routine amendments (see step 7)</td>
<td></td>
</tr>
<tr>
<td>All reference to other individuals has been removed/redacted (see step 8)</td>
<td></td>
</tr>
<tr>
<td>No relevant data has been omitted unless it is exempt (see step 9)</td>
<td></td>
</tr>
<tr>
<td>Any complex terms of codes have been explained (attach as necessary) (see step 10)</td>
<td></td>
</tr>
<tr>
<td>All relevant data has been printed (enclosed) (see step 11)</td>
<td></td>
</tr>
<tr>
<td>Two copies are enclosed – one for the response; one for retention by DPO</td>
<td></td>
</tr>
</tbody>
</table>

Signed (Head of Dept/School): _________________________________

Date: ____________________