



**South Gloucestershire and Stroud College
South Gloucestershire and Stroud Academy Trust**

Data Privacy & Protection Policy

Policy Guidance for all Group Stakeholders: Responding to a Data Subject Access Request

**If you would like this document in an alternate format
Please contact the Human Resources Department**

Prepared by:	Gavin Murray
Job Title / Role:	Data Protection Officer
Ref. No.: QPG:141	Date of this version: 14 May 2019 Review date: 01 May 2020 (subject to any legislative change) Upload to External College website? Yes Upload to e-Campus? Yes

9. MANDATORY INITIAL IMPACT SCREENING



Completed by:

Gavin Murray	Assistant Principal	17/06/2019
I have read the guidance document: Completing a Policy Impact Assessment?		✓
If this policy has been up-dated, please tick to confirm that the initial impact screening has also been reviewed:		<input type="checkbox"/>

EQUALITY AND DIVERSITY IMPACT ASSESSMENT

Characteristic	This policy seeks to:	
Age	No appreciable impact	
Disability	Treat with equal dignity, all learners and staff; and monitor participation, performance and progress of learners and staff with disabilities and act to address inequalities.	
Faith or Belief	No appreciable impact	
Gender	No appreciable impact	
Race or Ethnicity	No appreciable impact	
Orientation	No appreciable impact	
Gender reassignment	No appreciable impact	
Economic disadvantage	No appreciable impact	
Rural isolation	No appreciable impact	
Marriage	No appreciable impact	
Pregnancy & maternity	No appreciable impact	
Carers & care leavers	No appreciable impact	
Vulnerable persons	Safeguarding children or vulnerable adults	
Please identify any sections of the policy that specifically seek to maximise opportunities to improve diversity within any of the College's stakeholder groups:	Section 3	
Please identify any sections of the policy that specifically seek to improve equality of opportunity within any of the College's stakeholder groups:		
Is there any possibility that this policy could operate in a discriminatory way?	<input type="checkbox"/>	✘
	If you have ticked yes (red), which characteristic will be most affected? Choose an item.	
If yes please confirm that the Policy has been sent for a full Equality & Diversity Impact Assessment, and note the date:	<input type="checkbox"/>	Click or tap to enter a date.

Note: if the policy does not seek to increase diversity or improve equality you should go back and review it before submitting it for approval.

MAPPING OF FUNDAMENTAL RIGHTS

Which United Nations Convention on the Rights of the Child (UNCRC), Right does this policy most protect:	Art. 17 Access to information Choose an item. Choose an item.
Which Human Right (HRA) does this policy most protect:	Art. 8 Right to private & family life Choose an item.

DATA PROTECTION & PRIVACY BY DESIGN SCREENING

Tick to confirm that you have considered any data protection issues as part of the design and implementation of this policy; and, that implementing this policy will <u>not</u> result in the collection, storage or processing of personal data outside of official College systems:	✓
Tick to indicated that this policy has or requires a Data Privacy Impact Assessment:	<input type="checkbox"/>

1. Introduction

South Gloucestershire and Stroud College Group recognises the right of access, commonly referred to as a subject access request or data subject access request (DSAR), which gives individuals the right to access their personal data. This guidance is designed to help staff to recognise and action an access request and should help individual stakeholders to understand how the College will respond to such requests.

For the avoidance of doubt this guidance should be read in conjunction with the College/Trust's Data Privacy and Protection Policy which can be accessed [here](#).

2. The data that an individual can access

A DSAR request entitles the data subject to **personal data only**, which is information relating to them as a natural living person, who:

- Can be identified or who are identifiable, directly from the information in question; or
- Who can be indirectly identified from that information in combination with other information.

Personal data includes special category (sensitive) data and data on criminal conviction and offences; but as these are considered to be sensitive, they are only processed by the College/Trust in limited circumstances.

Notes: Information about the College, the SGS Group or any affiliate company, Trust or other body is not personal data.

The College/Trust considers all subject access requests to relate **only** to the data held at the time the request was received; and,

The College/Trust will not disclose, when responding to a DSAR, any 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.

The College/Trust **will not disclose**, when responding to a DSAR, any information from which the data subject is not identifiable or cannot be identified.

Best Practice Tip:

Anonymising data can help reduce privacy risks by making it more difficult to identify individuals.

Personal data that has been truly anonymised is not subject to the GDPR nor can it be disclosed in response to a DSAR request, therefore:

College/Trust staff are expected to comply with the **principle of data minimisation** and not hold or create more than they need. Staff will, where possible, use College system (such as Pro-monitor) to communicate information about individuals and will avoid identifying anyone in an email, who is not a recipient of that email.

3. Recognising a DSAR request

The GDPR does not specify how to make a valid request. Therefore, an individual can make a subject access request to the College/Trust verbally or in writing. (It could also be made via social media) and does not have to be to a specific person or contact point.

The request does not have to include the phrase 'subject access request' or Article 15 of the GDPR, if it is clear that the individual is asking for their own personal data.

Remember, the College/Trust has a legal responsibility to identify that an individual has made a request and to handle it accordingly. Therefore, all staff must be vigilant in recognising requests.

Any member of staff who believes they have received a DSAR request must immediately log this by emailing DataPrivacy@sgscol.ac.uk. If you are unsure it is important that you check with the requester that you have understood their request or seeks guidance via DataPrivacy@sgscol.ac.uk.

Subject access requests can be complicated, and for that reason the College/Trust have a form that can be completed to help to clarify requests. That form is contained within schedule 5 of our Data Privacy and Protect Policy but a copy is attached at section 9 of this document.

If you think you have received a request it is important that you invite the individual to use the form (because this can speed up processing); but you **must** make it clear that **it is not compulsory**.

4. Does the College/Trust charge a fee to requestors

In most cases the College/Trust does not charge a fee to respond to a subject access request. If the College/Trust needs to charge a fee, that fee will be levied in line with the Data Protection (Charges and Information) Regulations 2018 and the requestor will be advised as soon as is practical, following receipt of their request.

5. How long does the College/Trust have to comply with a DSAR

The College/Trust will act on the subject access request without undue delay and will respond to requestors within one month of receipt of the request.

This time period will be calculated from **the day after we receive the request** (whether the day after is a working day or not) **until the corresponding date, 30 days later**. For example, if we receive a request on Saturday, March 30th. The time limit will start from the next day (March 31st) which means we will respond to the requestor (within 30 days) and by the latest, April 29th.

If the corresponding date falls on a weekend or a public holiday, the College/Trust will respond by the **next working day**.

The College/Trust may decide to extend the time to respond by a further two months if the request is complex or if we have received several requests from the same individual. If we decide to extend the time period, we will let the individual know within one month of receiving their request and explain why the extension is necessary.

Note: If a request is unfounded or excessive it **will be rejected** by the College/Trust. The College/Trust will assess the factors which may make responding to a DSAR a particularly onerous exercise using the assessment tool at section 10.

Anyone wishing to lodge a DSAR with the College/Trust is advised to review the factors that may render their request as unfounded or excessive before making that request.

The College/Trust will only ever release data, in response to a subject access request, if we are satisfied as to the identity of the person making the request. This means that we may ask for proof of identity.

6. What additional information will the College/Trust supply in response to a DSAR

When responding to a DSAR the College/Trust will also provide individuals with the following information:

- the purposes of processing;
- the categories of personal data concerned;
- the recipients or categories of recipient that personal data is disclosed to;
- the retention period for storing the personal data or, where this is not possible, the criteria for determining how long it will be stored;
- the existence of individual's 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 the data, where it was not obtained directly from the individual;
- the existence of automated decision-making (including profiling); and
- the safeguards provided if personal data is transferred to a third country or international organisation.

Note: much of this information is already contained within our privacy notice.

7. Requests made on behalf of others

The College/Trust can accept subject access request via a third party. In these cases, the College/Trust needs to be satisfied 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.

If the College/Trust receives a request from a third party the College/Trust will always seek evidence of any entitlement or will send a Data Subject Access Waiver to the data subject before responding to the request and **this will extend the 30-day response period.**

8. Process to be followed upon receipt of a DSAR

Time-frame	Actions	Links
Day 1	<p>All staff will, upon receipt of a data subject access request (a request for personal information) specifically the person who receives the request will:</p> <ol style="list-style-type: none"> 1. Notify the Data Protection Officer (DPO) that a request has been received, and whether the request was made verbally or in writing; 2. Forward written requests to the DPO; and, 3. Ask the requestor if they would like to complete the Assess Request Form) note: this is not compulsory. <p>Note: the person who received the request should not correspond with the requestor again (about the request) unless authorised to do so by the DPO or a member of the Executive Team.</p>	<p>Maximum time period: 24 hours</p> <p>Notify the DPO here: DataPrivacy@sgscol.ac.uk</p>
Day 2	<p>The Data Protection Officer will:</p> <ol style="list-style-type: none"> 1. Record the relevant date of receipt of the subject access request; 2. Acknowledge to the requestor that the request has been received and inform them of the relevant date of receipt; 3. Confirm with the requestor if they will be required to confirm their identify and, if so, how they can do this; 4. Notify the Head of Human Resources and the Group IT Director that a subject access request has been received; and, complete the DSAR assessment tool. 5. Notify the Executive and Senior Lead of the relevant curriculum or corporate area that a request has been received; and that they will be required to review it as the reviewing manager. Where this is not possible the Executive Team will appoint an appropriate reviewing manager. 	<p>Maximum time period 48 hours</p>
Day 3	<p>The appropriate functions (Human Resources, IT Services, MIS, SGS Wellbeing and Student Union etc.) will begin processing the request – <u>but will not read the data.</u></p> <ol style="list-style-type: none"> 1. The processed request will be page numbered and arranged into 2 ‘bundles’ a control bundle and a live bundle. 2. Within 5 working days or as soon as it becomes apparent, that an extension to the response period may be required’ the relevant Head of Function will inform the DPO. <p>Note: where possible bundles will be produced</p>	<p>Maximum time period 10 working days</p>

	electronically and stored securely on behalf of the nominated reviewing manager.	
Day 17	<p>The reviewing manager is required to review the live bundle to ensure that the bundle contains only personal information relating to the data subject (requestor).</p> <ol style="list-style-type: none"> 1. Where redactions are required (for example: for non-personal data or data that relates to another individual); the reviewing manager will redact the live bundle and record where redactions have been made on the control bundle. Note: recording redactions is an essential audit requirement. 2. As soon as the reviewing manager identifies any possible delay to their review (for example: because of the volume of records) the reviewing manager must contact the DPO immediately to discuss the need for an extension to the time limit. 	Maximum time period 5 calendar days (which can be extended by 5 calendar days with the consent of the DPO)
Day 18	The Reviewing Manager will pass the redacted bundle to the DPO who will discuss the redactions with the reviewing manager and add the additional supplementary information (see point 6 above) prior to notifying the data subject that the subject access request is ready for postage or collection.	
Day 27	<p>Where the reviewing manager has been granted an extension to the review time.</p> <ol style="list-style-type: none"> 1. The Reviewing Manager will pass the redacted bundle to the DPO who will discuss the redactions with the reviewing manager and add the additional supplementary information (see point 6 above) prior to notifying the data subject that the subject access request is ready for postage or collection. 	
Day 18-30	The DPO will contact the data subject (requestor) to confirm that the subject access request is ready for postage or collection.	



9. Data subject access request form

Schedule 5: SGS Data Privacy & Protection: Data Subject Request

Please provide the following details, which will help us to process your request.

You do not have to complete this form, but it may help us to respond more quickly to your request

The completed form can be sent to:

Data Protection Officer
SGS Stroud Campus
Stratford Road
Stroud
Gloucestershire
GL5 4AH

Or emailed to: DataPrivacy@sgscol.ac.uk

SURNAME	
FIRST NAME	
ADDRESS	
TELEPHONE	
EMAIL ADDRESS	

ARE YOU A STUDENT OR A FORMER STUDENT?	YES / NO
WHAT DID YOU STUDY AT SGS COLLEGE/ SGS AT	
YEAR OF REGISTRATION	
LEARNER ID NUMBER (IF KNOWN)	
YEAR OF LEAVING / COMPLETION	

ARE YOU A MEMBER OF STAFF OR A FORMER MEMBER OF STAFF?	YES / NO
STAFF ID NUMBER (IF KNOWN)	
WHAT DEPARTMENT(S) DID YOU WORK IN?	
YEARS EMPLOYED AT COLLEGE	
ANY INFORMATION THAT MAY HELP US	

Which Data Subject right(s) does your request relate to?

I would like to access my Personal Information held by SGS	<input type="checkbox"/>	Please indicate the information you wish to access:
		Please indicate the date range for your request (e.g. May 2018 to June 2018):
I would like to object to SGS Processing of my Personal Information	<input type="checkbox"/>	Please indicate the reason for your objection:
I would like to object to automated decision-making, by SGS, based upon my Personal Information	<input type="checkbox"/>	Please indicate the automated decision you wish to object to:
I would like to restrict Processing of my Personal Information by SGS	<input type="checkbox"/>	Please indicate the information you wish to restrict processing of:
I would like to port (transfer) my Personal Information from SGS	<input type="checkbox"/>	Please indicate the information you wish to port and to where:
I would like to request rectification of my Personal Information, held by SGS, which I believe to be inaccurate	<input type="checkbox"/>	Please indicate the information you wish to rectify and why:
I would like to request erasure of my Personal Data held by SGS	<input type="checkbox"/>	Please indicate the information you wish to erase:

Please note that these rights are not always absolute. If you are objecting to processing or automated processing or if you wish to restrict processing or ask that we erase data that we hold, we will review your request and respond to you within 30 day to inform you of our decision.

SIGNATURE: Date:

NAME (please print):

OFFICE USE ONLY

Date Request received	Request received by
Information Provided	
Signed	
Job Title	Date information provided
Request reference number:	

10. DSAR Assessment tool

Request reference number:	
Name of the Officer completing the assessment:	
DPO advise sought:	Choose an item.
Category of Data Subject:	Choose an item.

Has the specified the reason for their request?	
Yes, they wish to exercise their right to be informed of the personal data that the College holds and processes about them.	<input type="checkbox"/>
Yes, they wish to exercise their right to access (obtain a copy of) the personal data that relates to them and the College holds and processes.	<input type="checkbox"/>
Yes, they wish to exercise their right to rectify personal data that relates to them and the College holds and processes.	<input type="checkbox"/>
Yes, they wish to exercise their right to erase personal data that relates to them and the College holds and processes.	<input type="checkbox"/>
Yes, they wish to exercise their right to restrict processing of personal data that relates to them and that the College holds and processes.	<input type="checkbox"/>
Yes, they wish to exercise their right to right to port data that the College holds and processes about them to another Data Controller (within the EEA).	<input type="checkbox"/>
Yes, they wish to exercise their right to object to the College holding or continuing to process the personal data that it hold about them.	<input type="checkbox"/>
Yes, the data subject wishes to understand any automated decision making and profiling that the College does in relation to their personal data.	<input type="checkbox"/>

Factors affecting the reasonableness of the request:

The requestor has not specified the reason for their request:	1	2	3
<input type="checkbox"/>			
What time period does the request cover?	1	2	3
A period of up to 3 calendar months from today's date OR any period in the last academic years of no more than 3 calendar months.	<input type="checkbox"/>		
A period of up to 6 calendar months from today's date OR any period in the last academic years of no more than 6 calendar months.		<input type="checkbox"/>	
A period of up to 12 calendar months from today's date OR any period in the last academic years of no more than 12 calendar months.			<input type="checkbox"/>
Any period greater than 12 calendar months OR any unspecified period			<input type="checkbox"/>
How wide is the nature of the request?	1	2	3
The request specifies a single specific type of data (e.g. Personnel File/Educational Record)	<input type="checkbox"/>		
The request specifies a no more than two separate specific type of data (e.g. Personnel File/ Educational Record and Equalities Monitoring Data)		<input type="checkbox"/>	
The request does not specify specific types of data (in other words the request is wide ranging)			<input type="checkbox"/>
How many potential custodians (of the data subjects data) need to be contacted?	1	2	3
The requestor has specified the exact custodians	<input type="checkbox"/>		
The requestor has specified or there are no greater than 5 custodians		<input type="checkbox"/>	
The requestor has not specified or there are greater than 5 custodians		<input type="checkbox"/>	<input type="checkbox"/>
The requestor has specified and there are greater than 10 custodians			<input type="checkbox"/>
Is there likely to be a need to redact large amounts of third party personal data? (For example, the requestor has asked for a large	1	2	3

amount of records from many custodians such as emails)			
No	<input type="checkbox"/>		
Yes			<input type="checkbox"/>
There are relevant exemptions (to be completed with the DPO ONLY)	1	2	3
No	<input type="checkbox"/>		
Yes		<input type="checkbox"/>	<input type="checkbox"/>
How many systems need to be accessed?	1	2	3
The number of systems that need to be accessed and searched is restricted to two (for example: Personnel files, email archives, software applications used to store appraisals, HR information, payroll, Pro-Monitor, My Concern or Pro-Solution etc.).	<input type="checkbox"/>		
The number of systems that need to be accessed and searched is between two and five (for example: Personnel files, email archives, software applications used to store appraisals, HR information, payroll, Pro-Monitor, My Concern or Pro-Solution etc.).		<input type="checkbox"/>	
The number of systems that need to be accessed and searched is greater than five (for example: Personnel files, email archives, software applications used to store appraisals, HR information, payroll, Pro-Monitor, My Concern or Pro-Solution etc.).			<input type="checkbox"/>

Low	1 – 9	Medium	10 - 15	High	16 - 19
Total					

Advice/ recommendation of the Head of Human Resources <i>Head of HR to provide their view of the reasonableness of the request:</i>			
Advice/ recommendation of the Group IT Director <i>Group IT Director to provide their view of the reasonableness of the request:</i>			
Recommendation of the DPO:			
The request is not unfounded or excessive and should be granted	The requestor should be asked to refine the request	A two month extension is required to comply with the request	The request is unfounded or excessive and should be declined
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DPO Notes to the Data Controller:			
Decision of the Data Controller:		Singed:	

NOTE, it is clear that the data protection regulators expect data controllers to engage in dialogue with individuals making a DSAR, where the scope of the request is very wide, in the hope that it can be narrowed down whilst still satisfying the individual.