DATA SUBJECT ACCESS REQUEST PROCEDURE

Document Control Box	
Document title (include version number if amended within same year as approved)	Data Subject Access Request Procedure
Reference Number	009/21
Approval category (Please indicate)	
Governance/Governor	x
MPRIG Executive/Other Committee (insert name)	
Senior Staff (insert name)	
Date document approved	11 Feb 2019
Supersedes (insert previous title and/or version date)	11/2/19
Date document last reviewed and/or updated	25/3/21
Date next due for review	Feb 24
Related statutes or regulations	
Related policies/procedures/guidance/forms	DSAR Form DSAR Data Disclosure Form DSAR Case Log Template
Staff member responsible for update	Head of Compliance

Amendment History

Version	Revision Summary	Date Approved	Author
Feb 21	Appendix 3 added, GDPR law updated, weblink added, minor wording changes.		J Bradbury

Data Subject Access Request Procedure

Introduction

1. The UK General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA) provide individuals with rights in connection with the personal data held about them. It provides those individuals with a right of access to their data, subject to the rights of third parties and the satisfaction of a number of criteria. This procedure defines the process to be followed when a request for access to personal data is received.

Reference documents

- UK-GDPR (United Kingdom General Data Protection Regulation) January 2020. ...
- Spurgeon's College Data Protection Policy
- Data Protection Act 2018
- Spurgeon's College Information Rights Procedure
- Data Subject Access Request Form
- Data Subject Access Request Case Log
- Data Subject Access Request Data Disclosure Form

Responsibilities and definitions

2. **Data Protection Officer** (DPO) is responsible for ensuring that statutory and regulatory obligations with respect to the GDPR are adhered to. Where DPO is referred to, they may nominate a 'responsible person' to undertake some of their actions in regard to this procedure.

3. **Employees** are responsible for incorporating this procedure and its associated policy into their own working practices.

4. **Data Subject** is the person whose data is being requested

5. **Data Subject Representative** is an authorised person who is requesting information about or on behalf of the data subject

6. **Data Subject Access Request (DSAR)** is any request made by an individual or an individual's legal representative for information held by the College about that individual. The DSAR provides the right for data subjects to see or view their own personal data as well as to request copies of the data.

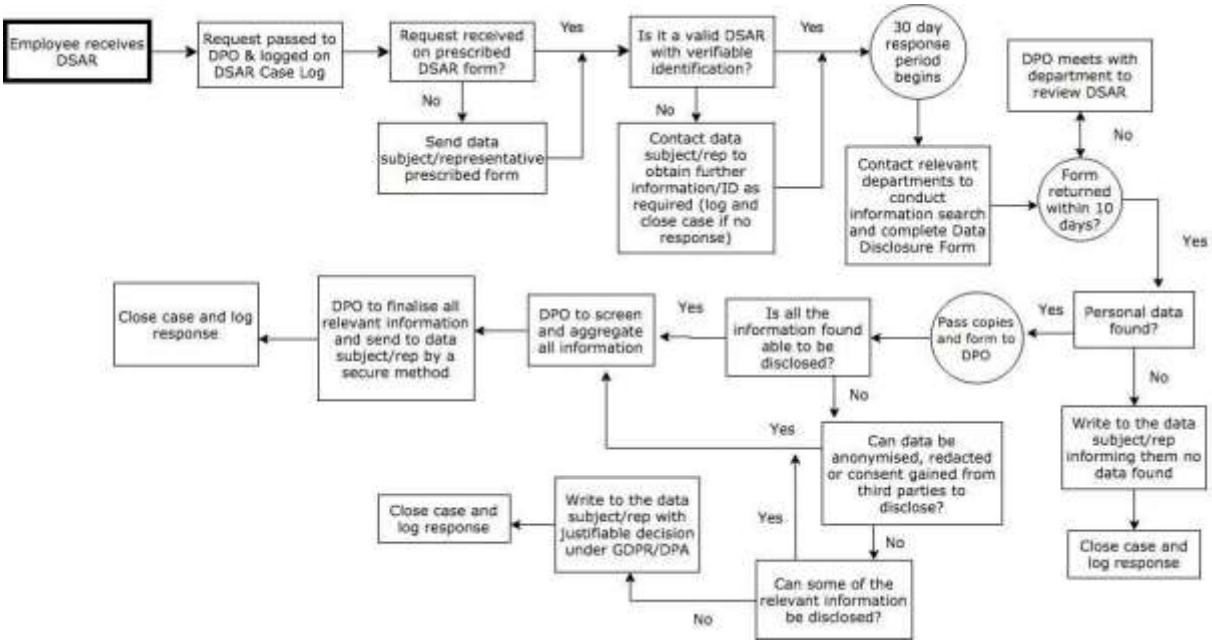
Data subject rights

7. The rights to data subject access include the following:
   - To know whether a data controller holds any personal data about them.
   - To receive a description of the data held about them and, if permissible and practical, a copy of the data.
   - To be informed of the purpose(s) for which that data is being processed, and from where it was received.
   - To be informed whether the information is being disclosed to anyone apart from the original recipient of the data; and if so, the identity of those recipients.
   - The right of data portability. Data subjects can ask that their personal data be transferred to them or a third party in machine readable format (Word, PDF, etc.). However, such requests can only be fulfilled if the data in question was provided by the data subject to the College, is processed automatically and is processed based on consent or fulfilment of a contract.
   - If the data is being used to make automated decisions about the data subject, to be told what logic the system uses to make those decisions and to be able to request human intervention.

8. Much of this information is provided to the data subject via the relevant College Privacy Notices.

9. The College must provide a response to data subjects requesting access to their data within **30 calendar days** of receiving a valid DSAR.

DSAR Process



Request

10. The GDPR does not specify how to make a valid request. Therefore, an individual can make a subject access request verbally or in writing, including on social media. It can also be made to any part of the College (including by social media) and does not have to be to a specific person or contact point. A request is valid if it is clear that the individual is asking for their own personal data. An individual does not need to use a specific form of words, refer to legislation or direct the request to a specific contact.

11. Upon receipt of a DSAR, employees must transfer the request to the DPO (or nominated deputy), who will acknowledge the request and the requestor will usually be asked to complete a 'Data Subject Access Request Form' if they have not done so.

12. This form provides the College with sufficient information to validate the identity of the data subject and to locate the relevant information being requested efficiently.

13. There is no legal requirement for the data subject to complete a form but in order to process a DSAR the College must be able to verify the identity of the data subject and have enough detail to be able to identify the information being requested.

14. The date of the initial request and the date the request form was sent should be logged on the 'DSAR Case Log' with a unique case reference number.

15. If the prescribed form or requested information is not returned within a reasonable time period then (provided the College is confident that the form was delivered and has undertaken reasonable follow up to ensure the data subject does not wish to pursue their right) the case should be closed and the response logged.

16. NOTE: The 30 day response period starts the day the data subject/requestor submits a valid DSAR with proof of identity that has been verified (see paragraphs 18-21).

17. If it is clear that the information being requested is 'complex or numerous' then the period of compliance may be extended for a further two months. In these circumstances the College must inform the data subject within one month of receipt of the request and explain why the extension is necessary.

Identity verification

18. The DPO needs to check the identity of anyone making a DSAR to ensure information is only given to the person who is entitled to it.

19. In the case of a request from current staff or students, the submission of the DSAR form with a verifiable signature and contact method may be enough. Generally, however, there will be a requirement for the data subject and requestor (if relevant) to provide identification. This must be a government

issued document containing a photo and/or a signature.

20. If the requestor is not the data subject, written confirmation that the requestor is authorised to act on behalf of the data subject is required, as well as validating the requestors identity.

21. If valid identification is not sent within a reasonable time period (provided the College is confident that the request was delivered and has undertaken reasonable follow up to ensure the data subject does not wish to pursue their right) the case should be closed and the response logged.

Gathering information

22. The DPO will contact relevant staff and provide them with the DSAR.

23. Staff should consider where 'personal data' about the individual concerned might be held, and conduct a search. Information may be stored electronically or in hard copy. It may be located in databases, filing systems (electronic and manual), student or personnel records, shared drives, the Intranet, College Social media accounts, email and/or filing systems of particular individuals, or with third party service providers. If necessary, colleagues many need to search their personal drives and e-mail accounts.

24. Information discovered should be recorded on the DSAR Data Disclosure Form, and the form and copies of the information returned to the DPO within 10 working days. The DPO may meet with staff to review progress and offer advice if required.

25. An electronic folder should be created for each DSAR – the filename should be made up from the reference number and surname of the applicant and should contain:
    - Copies of the correspondence between the DPO and the data subject and between the DPO and any other parties.
    - A record of any methods used to verify the identity of the data subject.
    - A record of the DPO decisions and how they came to those decisions.
    - Copies of the information sent to the data subject, including any anonymised or redacted versions sent.

26. Guidance on what constitutes personal data is contained in Appendix 1.

27. If no personal data is found then the DPO should be informed. A written response to that effect will be sent to the data subject/representative and the response logged.

Review of information

28. The DPO will determine whether there is any information which may be subject to an exemption and/or if consent is required to be provided from a third party

identified within the information (see section 6). Further guidance on how to review information is contained in Appendix 2.

29. The DPO must ensure that the information is received and reviewed in time to ensure the 30 calendar day timeframe is not breached.

30. A DSAR relates to the data held at the time the request was received. It is not acceptable to amend or delete the data if we would not otherwise have done so. Under the DPA, it is an offence to make any amendment with the intention of preventing its disclosure. However if routine use of the data may result in it being amended or deleted while dealing with the request (e.g. files are being routinely deleted in accordance with our records retention schedule), then it is acceptable to supply information as it is held when you send the response.

Response

31. The DPO will provide the finalised response together with the information retrieved from the department(s) and/or a statement that the College does not hold the information requested, or that an exemption applies. This response must be logged.

32. The DPO will ensure that a written response will be sent back to the requestor. This will be via email, unless the requestor has specified another method by which they wish to receive the response (e.g. post). The College will only provide information via channels that are relatively secure. When hard copies of information are posted, they will be sealed securely and sent by recorded delivery.

Exemptions

33. An individual does not have the right to access information recorded about someone else, unless they are an authorised representative, or have parental responsibility.

34. The College is not required to respond to requests for information unless it is provided with sufficient details to enable the location of the information to be identified, and to satisfy itself as to the identity of the data subject making the request.

35. In principle, the College will not normally disclose the following types of information in response to a DSAR:

    - Information about other people – A DSAR may cover information which relates to an individual or individuals other than the data subject. Access to such data will not be granted, unless the individuals involved consent to the disclosure of their data. (See Appendix 3 for further details)
    - Repeat requests – Where a similar or identical request in relation to the same data subject has previously been complied with within a reasonable

time period, and where there is no significant change in personal data held in relation to that data subject, any further request made within a six month period of the original request will be considered a repeat request, and the College will not normally provide a further copy of the same data.

- Publicly available information – The College is not required to provide copies of documents which are already in the public domain.
- Opinions given in confidence or protected by law – The College does not have to disclose personal data held in relation to a data subject that is in the form of an opinion given in confidence or protected by law.
- Privileged documents – Any privileged information held by the College need not be disclosed in response to a DSAR. In general, privileged information includes any document which is confidential (e.g. a direct communication between a client and their lawyer) and is created for the purpose of obtaining or giving legal advice.
- If the information is kept only for the purpose of statistics or research, and where the results of the statistical work or research are not made available in a form that identifies any of the individuals involved.
- Requests made for other, non-data protection, purposes
- Vexatious requests

36. If the DPO refuses a DSAR, the reasons for the rejection must be clearly set out in writing. Any individual dissatisfied with the outcome of their Data Subject Access Request is entitled to make a request to the College to review the outcome.

Documentation

37. Records of communications relating to a subject access request will be retained for 6 years.

Appendix 1 What is personal data?

I. The GDPR applies to the processing of personal data that is:

- wholly or partly by automated means; or
- the processing other than by automated means of personal data which forms part of, or is intended to form part of, a filing system.

II. Personal data only includes information relating to natural persons 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 may also include special categories of personal data or criminal conviction and offences data. These are considered to be more sensitive and you may only process them in more limited circumstances.
- Pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data.
- If personal data can be truly anonymised then the anonymised data is not subject to the GDPR. It is important to understand what personal data is in order to understand if the data has been anonymised.
- Information about a deceased person does not constitute personal data and therefore is not subject to the GDPR.
- Information about companies or public authorities is not personal data.
- However, information about individuals acting as sole traders, employees, partners and company directors where they are individually identifiable and the information relates to them as an individual may constitute personal data.

Appendix 2

Reviewing information - what can and cannot be disclosed as a result of a DSAR

I. Once all the information held about a data subject has been collected, it must be examined in detail to establish if it should be disclosed. This must be done on a case-by-case basis for each individual piece of information. In some cases only parts of particular documents should be disclosed.

II. It is the information and not copies of the documents that are legally required to be disclosed.

a. Check that the record is actually about the person concerned and not about someone else with the same name. Just because a record contains somebody's names does not always mean that it is about them. For example, an e-mail might carry the subject line "Meeting about John Smith" but if the e-mail only contains details about whether people can attend the meeting, the e-mail is not about John Smith.

b. Screen out any duplicate records. For example if there has been an e-mail exchange between colleagues, it is only necessary to print out the last e-mail in the exchange if copies of all the other e-mails are part of the last e-mail.

c. If a record was created by a member of staff acting in a private rather than an official capacity, only exceptional circumstances would justify its disclosure without their consent. If they are not prepared to disclose the record, do not disclose it.

d. The College should only disclose information which is about the person making the subject access request. Where a document contains personal data about a number of individuals, including the data subject, they should not disclose the information about the third parties to the data subject. If the record is primarily about the data subject, with incidental information about others, they should redact the third party information. If the record is primarily about third parties, withhold it if redacting is not possible. Alternatively, contact the third party to obtain consent to disclose the document if possible. Ensure that any and all correspondence in these matters is logged.

e. The records may contain correspondence and comments about the data subject from a number of parties, including private individuals, external individuals acting in an official capacity, and College staff. In these cases we are required to balance the interests of the third party against the interests of the data subject and often omit or redact third party information.

f. Do not disclose information which would prejudice the prevention or detection of a crime. For example, if the Police informed us that a member of staff is under investigation, but the member of staff did not know this, then we should not provide that information to the member of staff whilst the investigation is in progress. However, if the investigation is closed or if the member of staff has been informed that there is an investigation underway, then the information should be disclosed in response to a subject access request.

g. Do not disclose any records which contain advice from our lawyers, where we are asking for legal advice or which were written as part of obtaining legal advice.

h. Do not disclose information which is being used, or may be used in future, in negotiations with the data subject if the information gives away our negotiating position and disclosing the information would weaken that negotiating position.

III. The exemptions identified above are those most likely to apply to information held by the College. There are others, and it is good practice to check the Information Commissioners Office website for up to date information regarding exemptions before responding to a DSAR. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/. Advice should be sought when it is thought that another exemption may be applicable.

IV. If the DPO discovers material which does not reflect favourably on the College (e.g. they may find documents which show that standard procedures have not been followed, or documents which may cause offence to the data subject), these documents must be disclosed. However, the DPO should bring their contents to the attention of the relevant manager and ensure that appropriate action is taken to address any issues that may arise.

V. Staff must not destroy or refuse to disclose records. This is a criminal offence if it is done after you know a subject access request has been made.

VI. Once all of the information that can be sent in response to a DSAR has been collated, one final review of this information as a collection must be made. This is to offset the risks often discovered by aggregating information. For example, the DPO may have identified that all the information they intend to release is unrestricted in its nature. However, once aggregated there is an inherent risk that additional information could be disclosed or at least interpreted. This has to be taken into consideration before the final response is made.

Appendix 3 Third Party Information

Responding to a subject access request may involve providing information that relates both to the individual making the request and to another individual. However, the DPA 2018 says that organisations 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.

In determining whether it is reasonable to disclose the information, the College must, however, take into account all of the relevant circumstances, including:

- the type of information that you would disclose;
- any duty of confidentiality you owe to the other individual;
- any steps you have taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

So, although the College may sometimes be able to disclose information relating to a third party, it needs to decide whether it is appropriate to do so in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to the College disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, the College must decide whether to disclose the information anyway. For the avoidance of doubt, the College cannot refuse to provide access to personal data about an individual simply because it has obtained that data from a third party.

The rules about third party data apply only to personal data which includes both information about the individual who is the subject of the request and information about someone else.