



John Moores Students' Union

Subject Access Request (SAR) Policy

Approved by the Trustee Board	10/07/2026
Date of Next Review	10/07/2029
Author	CEO & Deputy CEO

Charity Registration Number: 1202881

ICO Registration Number: ZB694682

Contents

	Page
Scope	3
What is the right of access?	3
General principles of responding to Subject Access Requests	3
How to recognise a Subject Access Request?	4
Procedure for responding to the request	5
Can a third party request an SAR?	6
Inspection & Audit Review	6
Related Policy	6
Annex A – Simple guide on redaction of information	7

1. Scope

This document applies to the employees, staff, workers and any other individuals working or undertaking a role under or on behalf of Liverpool John Moores University Students' Union (JMSU). When the terms 'we', 'us', 'our', the abbreviation 'JMSU', 'the Union' or 'the organisation' are used, it should be read as referring to Liverpool John Moores University Students' Union.

The UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018 ("DPA 2018") provides data subjects with a variety of rights in relation to the personal data held about them. For an overview of all the rights, please view our privacy notice/data protection policy, which can be accessed [here](#).

This policy specifically covers Article 15 of the UK GDPR – right of access.

2. What is the right of access?

The purpose of a Data Subject Access Request (DSAR or SAR) is to allow individuals to confirm the accuracy of personal data, check the legality of processing to allow them to exercise rights of correction or objection if necessary, and also request to see any personal data that we hold about them.

It should be noted that when responding to data subject access requests, data subjects are entitled (unless an exemption applies) to be informed of the following:

- a) Confirmation that personal data about them is being processed.
- b) A copy of that personal data.
- c) Details of the purpose of the processing.
- d) Categories of the personal data concerned e.g. does it include any special categories or sensitive personal information?
- e) The period the personal information will be stored for, or what the criteria is for determining the period of storage.

Members of staff should consult JMSU's Data Protection Officer on jmsu-dpo@ljmu.ac.uk if they receive a data subject access request. The Data Protection Officer shall be the person responsible to deal with and respond to such SARs.

As a general rule, personal data relating to other individuals should not be disclosed unless their permission has been obtained to release it, or it is reasonable to comply without consent. Therefore, if this is within the requested information, we should generally redact such information. Please see **Annex A** for more information on redaction of information.

3. General principles of responding to Subject Access Requests

3.1 COMMUNICATION

- 3.1.1 Any communication with the data subject when responding to any request must be in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- 3.1.2 Communication should be in writing, or by other means if appropriate e.g. electronic means. It can also be provided orally if requested by the data subject, provided that the organisation is satisfied of the identity of the data subject, and this is proven by other means. Where the request is by electronic

means, the information should be provided electronically where possible, unless otherwise requested by the data subject.

3.2 TIMING FOR RESPONSE

- 3.2.1 Any Subject Access Request must be dealt with promptly, and in any case **within one month** of receiving the request. If ID verification is requested, the time scale for responding does not begin until the organisation receives the requested information (however, the organisation must request ID documents promptly). JMSU will provide their response on the equivalent date in the following month, or earlier if the month is shorter and there's no equivalent. During this month, the organisation will keep the data subject informed of progress. Any delays caused by the data subject may be added to the month.
- 3.2.2 There may be some circumstances where JMSU can take longer than one month to fulfil the request, up to a **maximum two further months** where the request is complex, or if the organisation receives a high number of requests from the same individual e.g. other types of requests relating to individuals' rights. However, these circumstances are limited, and JMSU should always strive to meet the one-month timeframe wherever possible. If the Union needs to extend the response deadline, it must inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. The time limit takes no account of working days.

3.3 COST

- 3.3.1 In conjunction with UK GDPR, the organisation doesn't charge any fee when providing a copy of personal data undergoing processing. However, for any further copies requested by the data subject the organisation may charge a reasonable fee based on administrative costs. Furthermore, the organisation may be able to charge a fee when the requests are manifestly unfounded or excessive, in particular because of their repetitive character. In this case, JMSU will have to demonstrate how the request is manifestly unfounded or excessive in character and can either charge a reasonable fee taking into account the administrative costs of providing the information or communication, taking the action required or refuse to act on the request.

3.4 RESPONSIBILITIES

- 3.4.1 The Data Protection Officer is the internal responsible individual who oversees the SAR procedures.

4. How to recognise a Subject Access Request?

- 4.1 In order to identify a Subject Access Request, please be aware of the following aspects:

- a) SARs can be made verbally or in writing, including by social media (via Facebook, Instagram etc). However, it is not appropriate to use social media to supply information in response to a SAR for information security reasons. Instead, you should ask for an alternative delivery address for the response.
- b) SAR forms can make it easier for data subjects to submit requests, however, they are not compulsory.
- c) Data subjects can make their request to any part of your organisation, they do not have to direct it to a specific person or contact point.
- d) A request does not have to include the phrases 'subject access request', 'right of access' or 'Article 15 of the UK GDPR'.

- e) A request may mistakenly refer to other legislation, such as the Freedom of Information Act 2000 (FOIA) or the Freedom of Information (Scotland) Act 2002 (FOISA), but it's still valid as long as the individual is asking for their own personal data.

5. Procedure for responding to the request

- 5.1 **Passing on the request:** once an employee receives a SAR, they will inform their line manager and the data protection officer as soon as possible. The data subject may have completed an SAR request form, expressed their request verbally or in writing. (The organisation will accept any request from a data subject for access, including one made verbally - please refer to section 4 for more info)
- 5.2 **Assessing responsibilities:** the Data Protection Officer should assess if the SAR involves data for which JMSU is the Data Controller. If JMSU is a Data Processor, please inform the Data Controller, refer to the contract signed with them and follow their guidance. Otherwise, please refer to the following points.
- 5.3 **Acknowledgement of SAR:** JMSU should acknowledge receipt of a data subject request and confirm that the Union is looking into the request and will respond within the statutory timeframe.
- 5.4 **Verification of identity if required:** if JMSU has concerns over the identity of the person making the request, the Union may request the provision of additional information necessary to confirm the identity of the data subject, which has the effect of 'stopping the clock'. JMSU would not be obliged to respond to the request until it is satisfied of the identity of the person (acting reasonably). Please note it is possible that JMSU may receive requests from a third party on behalf of a data subject e.g. a solicitor or a power of attorney or a friend. In these cases, the Union 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. This might be a written authority to make the request, or it might be a more general power of attorney. For more information, please refer to section 6.
- 5.5 **Assessing whether extension required:** the Data Protection Officer will assess whether to extend the deadline to respond to the request and/or whether it needs additional information before responding, and communicate this to the data subject as soon as possible and no later than one month following receipt of the request.
- 5.6 **Identify relevant personal data:** identify the data that has been requested in the SAR and gather it. The organisation will provide a copy of the personal data held on the data subject, but it might not be provided in the format or document in which it is held.
- 5.7 **Identify data that needs to be redacted:** once the organisation has assembled the information to be presented to the data subject, this information may need to be redacted if it includes any personal data about someone other than the original data subject, in order to comply with Article 15.4 of the UK GDPR. The organisation will pay particular attention to not affect the rights or freedoms of others, including trade secrets or intellectual properties such as copyright.
- 5.8 **Refusing an SAR:**
 - a) the organisation may refuse to provide the information to the data subject if an exemption (Schedules 2 and 3 of the Data Protection Act 2018) applies. Please see Annex 2 for more information on exemptions.
 - b) A SAR may also be refused if the request is manifestly unfounded or excessive. A manifestly unfounded request might be intended to cause disruption or is clearly prompted by malice. A manifestly excessive request should be clearly unreasonable. JMSU should consider whether the

request is proportionate when balanced with the burden or costs involved in dealing with it. It must take into account the circumstances of the request, including: the nature of the requested information and the context of the request; whether a refusal to provide the information may cause substantive damage; its available resources; whether the request largely repeats previous requests and a reasonable interval hasn't elapsed; whether it overlaps with other requests.

- c) Each request should be considered on its own merit and on a case-by-case basis. If the organisation refuses to comply with a request, they will inform the individual of the reasons why, their right to make a complaint to the organisation, escalate this complaint to the ICO or another supervisory authority if they are unhappy with our response to their complaint, and their ability to seek to enforce this right through the courts.
- d) If, having considered the data subject request, JMSU decides that an exemption applies only in part, it should communicate its response to the data subject within the statutory timeframe and provide the necessary information with the non-disclosable information redacted where appropriate. The data subject should be informed of their right to complain to the organisation, escalate this complaint to the ICO if they are unhappy with our response, and their right to seek a judicial remedy.

5.9 **Processing the request:** if there is no exemption applicable and the request is not manifestly unfounded or excessive, the SAR will be processed.

5.10 **Recording responses:** Data Subject Access Requests must be tracked and recorded by JMSU in the 'Activities, Incidents and Risks log' for accountability purposes.

6. Can a third party request an SAR?

6.1 If you receive an SAR from a third party, you need to be satisfied that the third party making the request is entitled to act on behalf of the individual. It is the third party's responsibility to provide you with evidence of this. For example, by providing a written authority signed by the individual, stating that they give the third party permission to make a SAR on their behalf

6.2 If there is no evidence that a third party is authorised to act on behalf of an individual, you are not required to comply with the SAR, however you should still respond to them explaining this

6.3 In reference to the data of a child, remember that the data is effectively of the child. A parent/guardian doesn't have a specific right to obtain their child's data. If you obtain a request from a parent, it is the Data Protection Lead's decision as to whether such information must be disclosed, and must consider that the child should themselves exercise such a right if they are competent.

7. Inspection & Audit Review

7.1 This Policy is updated regularly by the Data Protection Officer when required. It is reviewed annually by the Data Protection Officer and the Board of Trustees.

7.2 An annual report on data protection will be produced by JMSU for consideration by the Board of Trustees. This report will include information to help the Trustee Board compare JMSU's decision-making over time.

7.3 The job titles referred to in this Policy are subject to change. If there is any doubt about designated roles, final clarification will be given by the Chief Executive.

8. Related Policy

8.1 This policy should be read in conjunction with the following policies and documents:

- a. Data Protection policy
- b. Confidentiality agreement
- c. Privacy notice
- d. IT terms and conditions

8.2 JMSU Policies can be found at <https://www.jmsu.co.uk/what-we-do-how-we-work/our-policies>

9. Annex A – Simple guide on redaction of information

Information relating to another individual that has no association with the data subject	→ This is likely to be redacted unless you have the consent of the other individual. <i>If the consent cannot be sought/obtained, has been refused or the request for consent has not been responded to, then consider is it reasonable in all the circumstances to disclose the information without consent?</i>
Information related to the data subject provided by an external individual or by a third-party organisation	→ This is likely to be redacted unless you have the authorisation of the other individual/third-party organisation. <i>If the authorisation cannot be sought/obtained, has been refused, or the request for authorisation has not been responded to then consider is it reasonable in all the circumstances to disclose the information without authorisation?</i>
More in general, if the information disclosed was already known to the data subject	→ This is unlikely to be redacted
Information relating to another individual that was provided by the data subjects themselves (e.g. summary of a 1:1 between the data subject and staff, where the data subject spoke about another individual)	→ This is unlikely to be redacted
If any information raises general concerns in terms of confidentiality, safeguarding or any risk of prejudice of social work and prevention of crime	→ This will require an internal conversation amongst professionals to decide if it's reasonable or not to disclose the information. <i>To understand if it's reasonable to disclose information, you may want to consider reflecting (if applicable) on the following questions:</i> • <i>is there a duty of confidentiality to any of the persons identified e.g., would the information have been provided in an expectation of confidentiality, in relation to health, lawyer, financial, police, social worker, teacher, etc?</i> • <i>Is there a public interest case in disclosing the information?</i> • <i>Is the information already in the wider domain or known to the data subject?</i> • <i>Is there a risk of harm to any parties or risk of prejudice of social work or detection/prevention of crime?</i>