
Data Subject Access Request Procedure

Responsible Office	Governance, Legal & Compliance
Responsible Officer	University Secretary
Approval authority	University Secretary (in consultation with the Information Governance Group)
Date of approval	January 2023
Amended (if applicable)	n/a
Related University Policies	Data Protection Policy
Related Procedures	
Effective Date	January 2023
Supersedes	(New)
Next review due	January 2028

1 Background

1.1 Bath Spa University is committed to protecting the rights and privacy of individuals ('data subjects') in accordance with UK data protection laws. Under the UK data protection laws, individuals have the right to be told what personal data the University is processing about them and, unless an exemption applies, to receive a copy of that information. Data subjects do this by making a **data subject access request (DSAR)**.

1.2 A DSAR may be received by anyone at the University, but it will be managed by the Information Compliance Manager, with oversight from the Data Protection Officer and assistance from relevant University staff and advisers.

1.3 All University staff should be aware of what a DSAR is, have a general understanding of what the University's obligations are to comply with such a request, and specific knowledge of their role and responsibilities in relation to a DSAR.

2 The Data Subject's Right of Access

2.1 A DSAR is any request made by an individual for personal data held by the University about that individual. A DSAR provides the right for data subjects to see or view their own personal data as well as to request copies of the data, unless an appropriate exemption applies.

2.2 In addition, an individual is entitled to receive further information about the University's processing of their Personal Data. This can normally be found in the University's privacy notices, which should detail the following:

- The categories of personal data being processed.
- The purpose(s) for which that data is being processed, and from where it was received.
- Whether the information is being disclosed to anyone apart from the original recipient of the data; and if so, the identity of those recipients.
- Any relevant safeguards that are in place when personal data is transferred to a third country.
- How long this data will be retained by the University.
- All data subject rights, as well as the right to complain to the Information Commissioner's Office (ICO).

2.3 A DSAR should be made in writing to the University, though it can also be requested verbally. There is no specific form in which a DSAR must be made. To assist individuals who wish to make a DSAR, the University has a DSAR form which is available on the [external website](#), but the use of this form is not mandatory. An individual does not need to use a specific form of words, refer to legislation or direct the request to a specific contact.

2.4 Prior to responding to a DSAR, the University must be certain of the identity of the requester (or the person the request is made on behalf of) and be sure that the information we hold relates to that individual. This is to ensure that personal data is not disclosed to a third party in error. The University may ask for sufficient information to enable it to judge whether the requester (or the person the request is made on behalf of) is the person that the personal data is about. If the request is made by a person on behalf of another (for example, a solicitor on behalf a client), the requester must provide sufficient evidence to satisfy the University that they are entitled to make the request and act on behalf of the data subject.

2.5 The University cannot charge a fee for processing a DSAR.

2.6 The University has one calendar month to provide a response to the requester. This is set by the UK GDPR, and the University is unable to extend it, except in very limited circumstances, such as when a request is complex. In this situation, the University may be able to increase the timeframe within which to respond to the individual by a further two calendar months.

2.7 Failure to comply with a DSAR can be serious and may result in the following:

- Individuals have the right to compensation if they are damaged by a breach of Data Protection law, for example if we fail to supply them with the information they request within the one calendar month time limit, and their interests suffer as a result.
- Individuals may complain to the ICO about any decision we make regarding the disclosure or non-disclosure of their information. The ICO may serve an enforcement notice ordering us to release the information and can also impose a substantial fine on the University.
- It is a criminal offence for an individual, be it a current or former member of staff, to erase, modify or fail to provide any information that has been requested for a DSAR.

3 Roles and Responsibilities

3.1 **University:** as a Data Controller, the University has a legal obligation to comply with any data subject access requests it receives.

3.2 **All University staff and authorised University representatives** are responsible for:

- immediately sending any correspondence that they believe could be a data subject access request to data-protection@bathspa.ac.uk;
- directing any individual enquires about how to make a data subject access request to the [Data Protection](#) pages of the University website;
- complying with the instructions of the Information Compliance Manager and/or Data Protection Officer in respect of any DSAR;
- seeking guidance and assistance regarding DSARs from the Information Compliance Manager;
- communicating to the Information Compliance Manager any concerns about the disclosure of any information in response to a DSAR.

3.3 The **Information Compliance Manager** is responsible for:

- processing and responding to any DSARs received by the University;
- providing instructions and advice to University staff on how to search for the requested information and consider any relevant exemptions which may be engaged.
- responding to queries relating to data subject access requests;
- seeking guidance and assistance regarding DSARs from the Data Protection Officer as required and implementing any steps required by the Data Protection Officer with regard to DSARs.

3.4 The **Data Protection Officer** is responsible for:

- ensuring that statutory and regulatory obligations with respect to Data Protection legislation are adhered to;
- providing oversight and advice where necessary in relation to data subject access requests.
- determining whether it is necessary to seek external, independent advice in the event of any complex or contentious data subject access requests, or (where necessary) for responding to complaints.

PROCEDURE

A. Receipt of DSAR and Initial Steps

1 Any DSAR submitted via the University's form will automatically be forwarded to the inbox data-protection@bathspa.ac.uk, which is monitored by the Information Compliance Manager.

2 If any University staff member receives a request from an individual for their own personal data and it is not a type of request that they would deal with as a routine part of their daily job (for example, if they work in a School administration role and the student wants to find out their module results), then they must immediately forward the request to data-protection@bathspa.ac.uk. If they

are not sure whether a request is a DSAR, the correspondence should be forwarded to data-protection@bathspa.ac.uk for advice from the Information Compliance Manager.

3 Once the request has been received/forwarded, it will be processed by the Information Compliance Manager. They will take initial steps to assess the DSAR, which may include:

- determining whether the request is a valid DSAR;
- (where applicable) contacting the requester for proof of identification. The statutory time period to respond does not begin until this has been received by BSU;
- asking the requester for further detail to assist with locating the personal data they are requesting and seeking clarification on the information they wish to obtain. The statutory time period to respond is paused and resumes again from this point upon receipt of a response from the requester;
- assessing relevant University departments and teams which may hold the personal information requested;
- considering whether an extension may be applied to the statutory time limit for response due to the complexity of the DSAR;
- Logging the DSAR.

B. Collation of Personal Data

4 Once the initial steps have been completed, the Information Compliance Manager will contact relevant University staff to request that the specified information is made available, confirm the timescale for a response and provide instructions on how any information should be collated and sent to the Information Compliance Manager.

5 When asked to assist with a DSAR, University staff must consider where personal data about the individual concerned may be held and undertake appropriate searches. 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, University social media accounts, email and/or filing systems of particular individuals, or with third party service providers. If necessary, colleagues may need to search their personal drives and e-mail accounts. **All records held by staff in their capacity as University employees are potentially disclosable in response to a DSAR.**

6 The Information Compliance Manager can provide additional guidance on searching email and other electronic records for staff who require this assistance.

7 Relevant University staff must send copies of any and all information retrieved to the Information Compliance Manager within the timeframe specified and in accordance with the instructions provided by the Information Compliance Manager.

8 Relevant University staff must raise any concerns about disclosure to the Information Compliance Manager as soon as possible, and at the latest upon the date on which the information is sent to the Information Compliance Manager. This includes any concern that the information should not be disclosed because one of the exemptions applies (see below). For clarity, all information must still be shared with the Information Manager to allow informed decisions to be made.

C. Review of Collated Personal Data

9 The Information Compliance Manager, with assistance from the Data Protection Officer if necessary, will review all information provided to ensure that it is appropriate for release to the requester. This will involve checking for any third party personal data, which can be any information that could potentially identify someone else, such as name, things they have said and their opinions.

10 All information that is not relevant to the requester, or which is third party personal data, will be redacted (removed or blocked out).

11 The Information Compliance Manager will consider the additional exemptions which may be engaged in other limited circumstances and decide whether any of these apply to the DSAR. These include, but are not limited to, the following:

- Legal professional privilege, which can apply to correspondence between solicitor and client for the purpose of obtaining legal advice and confidential communications made for the purpose of providing or obtaining legal advice about proposed or contemplated litigation.
- Management forecasts, which can apply when an organisation is making decisions about its future but it hasn't yet finalised these or communicated them to members of staff. This may be the case when the organisation is planning a restructure or a round of redundancies.
- Negotiations, which can apply when there are ongoing negotiations between the organisation and a data subject and to provide this information would prejudice these.
- Confidential references, which can apply to any confidential references which have been given or received by the organisation. This is only applicable if the reference was made in confidence and it is not a blanket exemption.
- Exam scripts and exam marks, which only applies to personal data contained within exam scripts. This means individuals do not have the right to copies of their answers to the exam questions. However, the information recorded by the person marking the exam is not exempt from the above provisions and may be provided when it is suitable to do so.

12 Once a review of the information has been completed by the Information Compliance Manager and all appropriate redactions have been applied, it may be necessary to consult with the Data Protection Officer or seek external legal guidance (for example, on complex or contentious requests or for advice on the application of an exemption).

D. Response to DSAR

13 When the information is ready for release it will be made available to the requester electronically (unless they state otherwise). This will normally be by way of a secure link to a drive or, if size allows, it can be sent as a password-protected email attachment to the email address specified by the requester.

14 The statutory time limit for providing a response to the requester is **one calendar month from the date the DSAR was received by the University**. In certain circumstances, such as when a DSAR is complex, this can be extended by a further two calendar months. However, the requester must be informed of the University's intention to apply the extension within one calendar month of making the DSAR.

15 The Information Compliance Manager will update the Log with the details of the release and retain an electronic copy of the information released on a secure drive.

E. Complaints

A requester has the right to complain to both Bath Spa University and the Information Commissioner's Office if they are unhappy with any aspect of their DSAR response.

16 Any University staff member who receives any correspondence which may be a complaint of this nature must send it to data-protection@bathspa.ac.uk immediately.

17 The Data Protection Officer will review any complaints received by the University regarding any aspect of a DSAR response, provided that they have not already been consulted on the DSAR at the Review stage (see section C above). If the Data Protection Officer has been involved at the Review stage, the Data Protection Officer may appoint an independent person to deal with the complaint (which may be an external person).

18 Complaints to the ICO about any aspect of the University's response to a DSAR may be submitted via the ICO's website: <https://ico.org.uk/make-a-complaint/>

APPENDIX: DATA SUBJECT ACCESS REQUEST PROCEDURE

