v2.0

Data Subject Access Requests and Rights Procedure

1. Background

1.1 Bath Spa University (BSU) is committed to protecting the rights and privacy of individuals ('data subjects') in accordance with UK data protection laws. Under UK data protection laws, individuals usually 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 or SAR**).

1.2 In addition to making a DSAR request, data subjects also have other rights related to their personal data including the right to have inaccurate data corrected or deleted, to object to the processing or use of data, to be informed about its use, to limit how the data is used, to indicate the format or to have the data transferred, and to prevent automated processing of their data. Regardless of the right being exercised by an individual, at Bath Spa we refer to all these types of rights related requests as **data subject access requests (DSAR)**. Not all of these rights are absolute, so although someone can make a request, it doesn't always mean that it will be fulfilled.

1.3 Requests for another person's data, that is not made on behalf of the individual, are known within BSU as **personal data disclosure requests (PDDR).** There is an exemption in the Data Protection Act 2018 that says we do not have to comply with these, if doing so means disclosing information which relates to another individual, except where the other individual has consented to the disclosure or it is reasonable to comply with the request without the individual's consent.

1.4 A DSAR or PDDR may be received by anyone at the University, but it will be managed by the Information Governance team, with oversight from the Information Governance Lead and Data Protection Officer and assistance from relevant University staff and advisers.

1.5 All University staff should be aware of what DSARs and PDDRs are, have a general understanding of what the University's obligations are to comply with such requests, and specific knowledge of their role and responsibilities in relation to them.

2. The Data Subject's Right of Access

2.1 A DSAR is any request made by an individual, or on behalf of an individual with appropriate authority, for personal data. 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 supplementary information about the University's processing of their Personal Data, and this must be provided alongside

the DSAR response. This can normally be found in the University's privacy notices, which should detail the following:

- The categories of personal data being processed and, where the personal data has not been collected from the data subject, any available information as to the source.

- The purpose(s) for which that data is being processed, and from where it was received, if not from the individual.

- Whether the information is being disclosed to any other organisations, groups or anyone apart from the original recipient of the data; and if so, the identity of those recipients.

- How long this data will be retained by the University or, if that is not possible, the criteria used to determine that period.

- The individual's right to request rectification, erasure or restriction, or to object to processing, as well as the right to complain to the Information Commissioner's Office (ICO).

- Whether or not we have used automated decision-making (including profiling) and, if so, information about the logic involved, as well as the significance and envisaged consequences of the processing for an individual.

- Any relevant safeguards in place when personal data has or will be transferred to a third country or international organisation.

2.3 A DSAR can be requested verbally, but ideally it should be made in writing to the University. There is no specific form in which a DSAR must be made. An individual does not need to use a specific form of words, refer to legislation or direct the request to a specific contact so it is important that colleagues are able to recognise a DSAR and know to forward it to dataprotection@bathspa.ac.uk.

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 determine 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 In most cases, 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. If a requester can be specific about the personal data sought, this will help us to respond within the one calendar month timeframe.

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 suffer damage as a result of a breach of Data Protection law. 'Damage' includes both material damage e.g. financial loss and non-material damage such as distress or emotional harm.

- Individuals may complain to the ICO about any decision we make regarding the disclosure or non-disclosure of their personal information. The ICO may serve an enforcement notice ordering us to release the information, can impose a substantial fine on the University or undertake other action e.g. auditing.

- It is a criminal offence for an individual, be it a current or former member of staff, to alter, deface, block, erase, destroy or conceal information with the intention of preventing its disclosure to the person making a DSAR.

3. Other Personal Data Requestors

3.1 A Personal Data Disclosure Request (PDDR) is a request for personal data that is not made on behalf of an individual. These requests usually come from other government organisations e.g. DWP, the Police, local Councils checking student status, however they may also come from members of the public e.g. seeking CCTV footage following a road traffic incident.

3.2 These requests should be forwarded to the Information Governance team for advice.

4 Roles and Responsibilities

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

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

- Immediately sending any correspondence that they believe could be a data subject access request or personal data disclosure 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 Governance team and/or Data Protection Officer in respect of any DSAR or PDDR;

- Seeking guidance and assistance regarding DSARs and PDDRs from the Information Governance team;

- Communicating to the Information Governance team any concerns about the disclosure of any information in response to a DSAR or PDDR.

4.3 **The Information Governance team is responsible for:**

- Processing and responding to any DSARs received by the University and for advising on PDDRs, including responding where appropriate;

- 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 and other rights requests;

- Seeking guidance and assistance regarding DSARs and PDDRs from the Data Protection Officer as required and implementing any steps required by the Data Protection Officer with regard to DSARs or PDDRs.

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

- Providing advice and guidance to enable adherence to statutory and regulatory obligations with respect to Data Protection legislation;

- Providing oversight and advice where necessary in relation to personal data and rights related requests.

- In discussion with the Head of Legal, determining whether it is necessary to seek external, independent advice in the event of complex or contentious requests, or (where necessary) for responding to complaints.

PROCEDURE

A. Receipt of DSAR/PDDR and Initial Steps

1 Any DSAR/PDDR should be forwarded to the inbox data-protection@bathspa.ac.uk, which is monitored by the Information Governance team.

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 or PDDR, the correspondence should be forwarded to data-protection@bathspa.ac.uk for advice from the Information Governance team.

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

- Determining whether the request is a valid DSAR/PDDR;
- Where applicable, contacting the requester for proof of identification. The statutory time 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, as appropriate. The statutory time to respond is paused and resumes again from this point upon receipt of a response from the requester;
- Identifying 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/PDDR.

B. Collation of Personal Data

4 Once the initial steps have been completed, the Information Governance team will contact relevant University staff to request that the specified information is provided to the Information Governance team, confirm the timescale for a response

and provide instructions on how any information should be collated and sent to the Information Governance team, particularly for large volumes of information.

5 When asked to assist with a DSAR/PDDR, 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, archives and backups, the Intranet, University social media accounts, email and/or filing systems of particular individuals, or with third parties e.g. service providers. If necessary, colleagues may need to search their personal drives, e-mail accounts and other apps. **All records held by staff in their capacity as University employees are potentially disclosable in response to a DSAR/PDDR.**

6 The Information Governance team 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 Governance team within the timeframe specified and in accordance with the instructions provided by the Information Governance team.**

8 **Relevant University staff must raise any concerns about disclosure to the Information Governance team as soon as possible, and at the latest upon the date on which the information is sent to the Information Governance team.** 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 Governance team to ensure a complete record is held of information identified in case of a complaint to the regulator and to allow informed decisions to be made.

C. Review of Collated Personal Data

9 The Information Governance team 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 Information that is not relevant to the request, or which is third party personal data that it would not be reasonable in the circumstances to disclose, will be redacted (removed or blocked out) unless there is little harm in providing it e.g. it would be disclosable under the Freedom of Information Act or is already known to the requester.

11 The Information Governance team will consider the additional exemptions which may be engaged in other limited circumstances and decide whether any of these apply to the DSAR/PDDR. 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 Governance team and all appropriate redactions have been applied, it may be necessary to consult with other colleagues and/or to seek external legal guidance (for example, on complex or contentious requests or for advice on the application of an exemption).

D. Response to DSAR/PDDR

13 When the information is ready for release it will normally be made available to the requester electronically. 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 response must also contain a copy of the supplementary information in addition to a copy of the personal data itself. If this information is provided in one of our privacy notices, a link to or a copy of the privacy notice can be provided, provided that link is 'clickable' or provided in full to enable it to be entered into a browser.

15 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.

16 The Information Governance team will update the Log with the details of the release and retain an electronic copy of the information identified and disclosed in a secure drive, in accordance with agreed retention periods.

E. Complaints

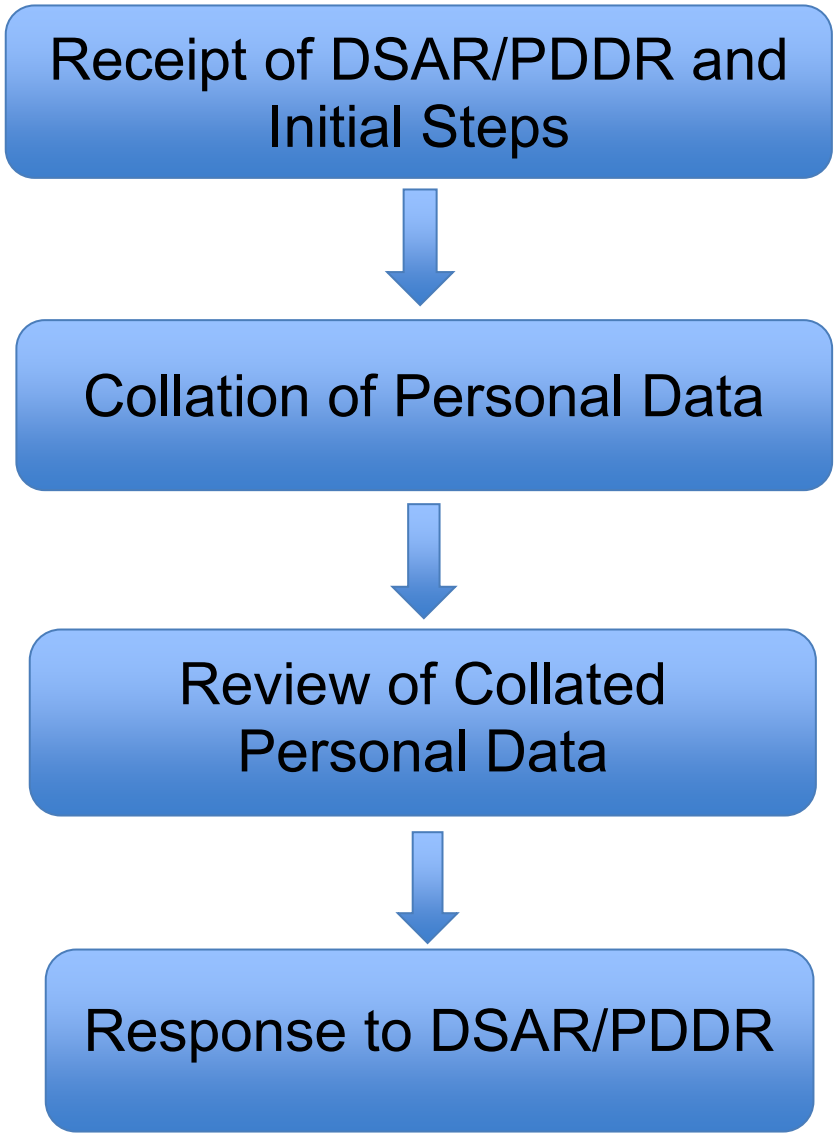
17 A requester may complain to both Bath Spa University and the Information Commissioner's Office if they are unhappy with any aspect of their DSAR response, however the complaint should go to BSU first to allow an opportunity to address the issue directly before going to the ICO. Requesters can also seek an effective judicial remedy (go through the courts) if their rights have been infringed.

18 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.

19 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, in consultation with the University Secretary, appoint an independent person to deal with the complaint (which may be an external person).

20 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



Document Details

Responsible Office: Governance, Legal & Compliance

Responsible Officer: University Secretary

Approving Authority: University Secretary

(in consultation with the Information Governance Group)

Date of latest approval: 26 June 2025

Effective Date: 26 June 2025

Related Policies and Procedures: Data Protection Policy

Supersedes: Data Subject Access Request Procedure January 2023 V1.0

Next review due: January 2028