Subject Access Requests: Guidance for staff

University Secretary
March 2019
Contents

1 Introduction ................................................................................................................................................. 3
2 The right to access personal data ................................................................................................................. 3
3 How should individuals make a request? ......................................................................................................... 3
4 What is an individual entitled to? ................................................................................................................. 4
5 Can we refuse to comply with a request? ........................................................................................................ 4
6 Can we charge a fee? ..................................................................................................................................... 4
7 Large amounts of personal data .................................................................................................................... 4
8 Exemptions .................................................................................................................................................... 5
9 Third party data ........................................................................................................................................... 5
10 Requesting Identification .............................................................................................................................. 6
11 Can someone act on behalf of the data subject? ......................................................................................... 6
12 Acknowledging a request .............................................................................................................................. 6
13 What to do if the request is not in writing ................................................................................................. 6
14 Timeframes for responding .......................................................................................................................... 6
15 Refusing a request ....................................................................................................................................... 7
16 How should we provide the information? .................................................................................................... 7
17 Response letter ............................................................................................................................................ 7
18 Sending the information ............................................................................................................................... 7
19 Record keeping ............................................................................................................................................ 7
Appendix A: Process Flowchart ....................................................................................................................... 8
Appendix B: Draft Response Letter ................................................................................................................ 9
Appendix C: Data records ............................................................................................................................... 11
1 Introduction

The University has a legal duty under Article 15 of the General Data Protection Regulations and the Data Protection Act 2018 to recognise and respond to subject access requests. This guidance has been produced to for staff who are responding to such requests.

Any questions about the process or a particular case should be referred to the University Secretary & Chief Compliance Officer. Please also see the University’s Data Protection Policy which is available here. Further information can also be found on the Information Commissioner’s website here.

Requests from staff members should be dealt with by HR and should be sent to HRServices@uwl.ac.uk. Requests from students will be dealt with by the Complaints and Compliance team and should be sent to university.secretary@uwl.ac.uk. Other requests should be referred to the University Secretary at the above email.

A flowchart which sets out the steps to be taken is set out in Appendix A. The sections below give explanatory detail.

2 The right to access personal data.

Individuals have the right of access to their data which is commonly referred to as subject access.

The University has one month to respond to a request, although in some circumstances the timeframe can be longer and the conditions for this are set out below.

3 How should individuals make a request?

The legislation does not specify how to make a valid request. A request can be made:

- orally or in writing.
- to any part of your organisation (including by social media) and does not have to be to a specific person or contact point

A request does not have to include the phrase 'subject access request' or reference Article 15 of the GDPR.

The University has a form which makes it easier for us to recognise and respond to subject access requests and the form is available here. However, although a form is helpful to clarify the request, we cannot require someone to use it.

You also cannot use completion of a form as a way of extending the one month time limit for responding.
4 What is an individual entitled to?

Individuals have the right to obtain the following from you:

- confirmation that you are processing their personal data
- a copy of their personal data
- a response within one month.

You must also provide:

- the purposes of your processing
- the categories and source of personal data
- disclosure
- retention periods
- the existence of their rights (including complaints to ICO)
- information about the source of the data;
- the existence of automated decision-making (including profiling); and
- the safeguards for transfers to a third country or international organisation.

You should send the response with a link to the Privacy Statement to confirm this additional information.

5 Can we refuse to comply with a request?

You can refuse to comply with a subject access request if it is 'manifestly unfounded or excessive'.

If you consider that a request is manifestly unfounded or excessive you can:

- request a "reasonable fee" to deal with the request (administrative costs only)
- refuse to deal with the request
- justify your decision and record it.

However, the normal expectation should be that we should try to respond to a request. There must be very good reason for refusing. Repeat requests may be a reason but they may be asking for different information. If you are considering refusing a request on the basis that it is excessive you should discuss this with the University Secretary.

6 Can we charge a fee?

Under the legislation, the University cannot charge a fee to deal with a request unless it is excessive. The University would only consider this in exceptional cases with the approval of the University Secretary. In most cases therefore there will be no fee charged.

7 Large amounts of personal data

If individuals ask for large amounts of data, we can ask them for more information to clarify their request. If we are going to do this, we need to let the individual know as
soon as possible that you need more information from them before responding to their request.

If we have asked for more information, the period for responding to the request begins when you receive the additional information.

However, if an individual refuses to provide any additional information, you must still endeavour to comply with their request (i.e. by making reasonable searches for the information covered by the request).

It should be noted that the ICO expect us to make extensive searches in order to comply with requests.

8 Exemptions

There are some exemptions that can be considered if the University is considering refusing a request. The most common reason is that it contains third party data and this is discussed in detail below. If you are considering refusing a request on other grounds, you should seek advice of the University Secretary.

In all cases you will need to justify the decision to apply the exemption. In some cases, such as commercial interests, you will need to apply a public interest test. Again the University Secretary or Head of Legal Services can advise or seek appropriate advice.

9 Third party data

You can only disclose information about a third party if:

• the other individual has consented to the disclosure; or
• it is reasonable to comply with the request without that individual’s consent

Staff data is generally in the public domain (e.g. you would disclose staff email addresses and also the emails from staff themselves unless it is about a personal matter).

As a general rule we will not disclose third party data, for example about students, unless it is deemed to be in the students’ best interests. This must be done on a case by case basis and the reasons for any refusal to disclose on this basis must be documented. This decision will involve balancing the data subject’s right of access against the other individual’s rights.

Where data has been provided on a confidential basis (e.g. a reference) this would also not normally be disclosed.

In determining whether it is reasonable to disclose the information, you must 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
• any express refusal of consent by the other individual.

10 Requesting Identification

Where the request is not from a current student or staff member, we should request identification from the data subject. We should do this as soon as possible and normally as part of the acknowledgement.

You should ask the data subject for birth certificate, driving licence, or passport and retain a copy of this before releasing the data.

11 Can someone act on behalf of the data subject?

It is acceptable to respond to a request from someone representing the data subject such as a solicitor or family member. However, the University must have the signed authority of the data subject in order to process the request.

12 Acknowledging a request

When you have received a request you should acknowledge the request within five working days. The acknowledgement should include confirmation that the University holds the data and any requests for clarification or identity documentation.

13 What to do if the request is not in writing

If the request is not in writing, you should write down the following:

• The name and contact details of the data subject
• The date of the request
• The information requested
• How the data subject would like to receive the data.

You should acknowledge the request and if possible get the data subject’s confirmation that what you have recorded is correct, for example, by asking them to confirm by return email.

14 Timeframes for responding

The University has one month to respond to a request.

The month starts on the day after the receipt of the request (regardless of whether this is a working day). For example, if the request is made on the 29 March, the University has until 30 April to respond. If there is no corresponding date, the request must be responded to by the last day of the month. For example, a request made on 30 January must be responded to by 28 February.

For the above reason, you should aim to respond to all requests within 28 days.
15 Refusing a request

You must inform the data subject as soon as possible and within one month of receipt of the request if you are going to refuse it.

You should inform the individual about:

• the reasons you are refusing the request, referring to the relevant exemptions;
• their right to make a complaint to the ICO or another supervisory authority; and
• their ability to seek to enforce this right through a judicial remedy.

16 How should we provide the information?

If requested electronically, you should respond electronically unless indicated otherwise.

Information should be in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

The information you provide in response to a request should be capable of being understood by the average person.

17 Response letter

There are various issues that you are required to set out in a response. A draft response letter is attached at Appendix B. If you need any help with the response you should ask the University Secretary or Head of Legal Services.

The template gives wording that you can amend as appropriate for the particular circumstances. It also sets out how you would set out the fact that some information is not being provided because it is confidential.

18 Sending the information

If you are sending the information via email, you should ensure that you send it as an encrypted PDF and send the password in a separate email. You should retain copies of the emails.

Information sent through the post should be sent by recorded delivery and confirmation of receipt should be retained.

19 Record keeping

A record should be retained of subject access requests and the response. A spreadsheet of the subject access requests made should be retained by the Department which dealt with them in the format attached at Appendix C.
Appendix A: Process Flowchart

Subject Access Request Procedure Flowchart

This flowchart describes the steps and decisions made in handling Subject Access Requests from when they are initially received.

1. **Request for access to information received**
   - Inform HR(Staff)/Compliance who will record the request in the SAR Log

2. **Can it be confirmed that personal data is held?**
   - **Y**
     - **Is the data subject’s identity clear?**
       - **N**
         - Discovery and collation of relevant personal data
       - **Y**
         - **Is it from a third party acting on behalf of the data subject?**
           - **Y**
             - **Is the third party’s authority to make a request clear?**
               - **N**
                 - **Request further information to verify authority to act for data subject**
               - **Y**
                 - **Review prepared data and redact if necessary**
           - **N**
             - **Request further information to verify identity**
     - **N**
       - **Does an exemption apply to any or all of the collated data?**
         - **Y**
           - **Review prepared data and redact if necessary**
         - **N**
           - **Update SAR Log to reflect response and decisions**

3. **Acknowledge receipt and confirm data held (if possible) within 3 working days**

4. **Can it be confirmed that personal data is held?**
   - **Y**
     - **Is the data subject’s identity clear?**
       - **N**
         - Discovery and collation of relevant personal data
       - **Y**
         - **Is it from a third party acting on behalf of the data subject?**
           - **Y**
             - **Is the third party’s authority to make a request clear?**
               - **N**
                 - **Request further information to verify authority to act for data subject**
               - **Y**
                 - **Review prepared data and redact if necessary**
           - **N**
             - **Request further information to verify identity**
     - **N**
       - **Does an exemption apply to any or all of the collated data?**
         - **Y**
           - **Review prepared data and redact if necessary**
         - **N**
           - **Update SAR Log to reflect response and decisions**

5. **Respond to data subject noting where any exemption has been applied, if applicable**

6. **Keep copies of response and data**
Dear X,

RE: Subject Access Request

We write further to your subject access request submitted on [xxxx], a copy of which is attached for ease of reference.

We can confirm that we have processed your personal data. For further information on the purposes of processing, the categories of data, how it is collected and who the data might be shared with, please see the [xxxx] privacy notice which is available here. The privacy notice also provides information on your rights with regard to this data, such as your right to request rectification and/or erasure of your data together with information on how data is stored, transferred, retained and protected.

Please find enclosed the information you requested. If the information is being sent by email, it will be encrypted and you will be sent a second email with the password.

To provide this information we have undertaken the following searches:

[insert information on searches provided]

[NOTE: Include details of the source of the data where it has not been obtained directly from the data subject]

We are unable to provide you with [xxxx]. This is because the information requested contains third party personal data.

The Data Protection Act 2018 Schedule 2 Part 3 section 16 (1) to (3) Exemptions from General Data Protection Regulation (GDPR) provides an exemption to disclosure of personal data if it contains third party personal data.

1. Protection of the rights of others – Data Protection Act 2018 (DPA 2018) Schedule 2 Part 3 section 16 (1) to (3) Exemptions from General Data Protection Regulation (GDPR)

**DPA 2018 Schedule 2 Part 3 section 16 (1) to (3)**

16 (1) Article 15 (1) to (3) of the GDPR (confirmation of processing, access to data and safeguards from third country transfers), and Article 5 of the GDPR so far as its provisions correspond to the rights and obligations provided for in Article 15(1) to (3), do not oblige a controller to disclose information to the data subject to the extent that doing so would involve disclosing information relating to another individual who can be identified from the information.
16 (2) Sub-paragraph (1) does not remove the controllers’ obligation where –
(a) the other individual has consented to the disclosure of the information to
the data subject, or (b) it is reasonable to disclose the information to the data
subject without the consent of the other individual.

16 (3) In determining whether it is reasonable to disclose the information
without consent, the controller must have regard to all the relevant
circumstances, including:
(a) The type of information that would be disclosed,
(b) Any duty of confidentiality owed to the other individual,
(c) Any steps taken by the controller with a view to seeking the consent of the
other individual,
(d) Whether the other individual is capable of giving consent, and
(e) Any express refusal of consent by the other individual.

The University has considered all the relevant circumstances of this matter as to
whether it is reasonable to disclose such information without consent of the third
party, and has concluded that it would unreasonable and a breach of its duty of
confidence this third party to disclose personal data without consent.

If you are unhappy with the way that the University has responded to your subject
access request, you may make a complaint to the University. The complaints
procedure is explained here. You may also complain to the Information
Commissioner and you can find details here.

Yours sincerely
Appendix C: Data records

<table>
<thead>
<tr>
<th>Department dealing with request</th>
<th>Name of data subject</th>
<th>Date of request</th>
<th>Deadline for providing data</th>
<th>Status (including date where completed)</th>
<th>Data subject type (Staff/Student/other)</th>
<th>Method of contact</th>
<th>Proof of ID needed</th>
<th>ID proof supplied</th>
<th>Confirmation of processing</th>
<th>Exemptions or restrictions</th>
<th>Format of response</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>