

## Subject Access Request (SAR) guidance for Heads/Principals

### Subject Access Requests

Individuals have a right to make a 'subject access request' (SAR) to gain access to personal information that Abbey DLD Group holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

A person can make a SAR for any reason and in any form. The request does not have to include the phrase 'subject access request' or make reference to the Data Protection Act, as long as it is clear that the individual is asking for their own personal data. Any member of staff can receive a SAR and so it is important they have training to know how to identify requests and the correct steps to follow.

For further information, see The Information Commissioner's Office guide which provides [very useful background information](#) and is essential reading for those who have to deal with SARs.

### Responding to a request

As outlined in the Group *Data Protection Policy*, if staff receive a subject access request they must immediately inform their Principal and e-mail the Data Protection Officer (DPO) at [DPO@abbeydld.co.uk](mailto:DPO@abbeydld.co.uk). Where possible, in their e-mail staff should include:

- The name of individual
- Their correspondence address
- Their contact number and email address
- Details of the information requested

Unless responsibility has been formally delegated to another member of the senior management team, responsibility for fulfilling a SAR lies with the Principal. The response to the data subject needs to be **within 1 month** of first receipt of the SAR. Heads/Principals should follow the procedure outlined below:

#### 1. Notification

The Principal should notify and seek advice from their line manager and the Group DPO (at [DPO@abbeydld.co.uk](mailto:DPO@abbeydld.co.uk)) as soon as a SAR is received. All SAR's must be logged on The Compliance Space.

#### 2. Application and Evidence of Identity

The Principal must send a standard letter of acknowledgment (see appendix 1) to the data subject and ask that, if they have not already done so, the data subject complete a SAR Request Form (see appendix 2). The data subject must, unless their identity is already verified by the Principal,

provide two forms of evidence as to their identity in the form of a current passport/driving license (signature to be cross-checked).

### Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children below the age of 13 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

### 3. Request Logged

The date of the identification checks and the specification of the data sought must be recorded in the SAR Log by the Principal.

In consultation with the DPO, the Head should determine whether the request meets any of the [exemption criteria](#) and the requester should be informed where a request cannot be fulfilled. Equally, if the request is unfounded or excessive, the school/college may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

Where a request is refused, the Principal must tell the individual why, and tell them that they have the right to complain to the ICO.

### 4. Discovery

All instances where the data subject's personal data is held must be discovered. This may entail searching all relevant databases and filing systems, including e-mails and readily available back up and archived files.

Where the data subject is a staff member, the search process will be split to allow for any personal data held by Head Office to be reviewed ahead of sharing with the school or Heads to ensure that no unnecessary or sensitive information is shared.

The Principal should identify whether support is required; for example:

- Technical help to search email, databases and network folders. Help should be requested from the Director of ICT.
- 'Editorial' and administrative help in identifying, reviewing and (where appropriate) redacting the relevant content. This should normally be performed by the School/College, unless there are reasons where objectivity or competence may be subject to doubt. Advice on this part of the process may be sought from the Principal's line manager, or the Group Data Protection Officer (via [DPO@abbeydld.co.uk](mailto:DPO@abbeydld.co.uk)).
- Legal help where the issues raised present a risk to the Group and are legally complex. Help should be requested from, and approved by the Principal's line manager.

Recognising the huge burden that SARs can place upon organisational resources, in practice it is reasonable and acceptable to:

- engage with the requestor to discuss the reason for the request, with a view to focusing the SAR on a particular topic,
- take a common-sense and practical approach to retrieving and presenting the data, as long as this is done in good faith and not with the intention of limiting the disclosure of data which may be pertinent to the request.

Under no circumstances must any documentation containing personal data pertaining to the data subject be amended or deleted after the SAR has been received, unless that amendment or deletion is part of a standard routine; for example, the overwriting of a daily rota. It is an offence to make any amendment with the intention of preventing its disclosure.

## 5. Response

The response to the data subject needs to be within **1 month** of first receipt of the SAR. Before the Principal sends the relevant information to the data subject, they must inform their line manager of any significant issues or risks that are likely to arise as a result of the SAR disclosure.

The response should be provided to the data subject in electronic format unless otherwise requested. It should be presented in a concise, transparent, intelligible and easily accessible form, using clear and plain language. This is particularly important where the information is addressed to a child.

The response should include the requester's name and the date on which the information is being delivered. It must specify whether or not you hold their personal data, a description of the personal data you hold, where it came from and why their data is being processed. If the data has been sent elsewhere you must also detail the recipients.

The Principal is responsible for ensuring all information is reviewed to identify whether any third parties are identified. Where third parties are identified, the Principal must either omit or redact their information from the response or obtain written consent from the third party for their identity to be revealed.

In all cases special care should be taken to redact all personal data or confidential information that the data subject should not see.

## Appendix 1 - Standard wording for response to a Subject Access Request

When responding it is advisable to do so in a non-confrontational and accommodating fashion, particularly if you are requesting further information prior to beginning your search. The ICO does allow you to filter to narrow your search and you can ask the individual to be more specific in their request. A template has been provided to assist with this in appendix 2. A blank copy of this can also be found on the portal.

-----

Dear [Insert name]

The information you have requested for [add in details] will be treated as a Subject Access Request in line with the Data Protection Act 2018. The statutory deadline for us to respond to your Subject Access Request is one month and we will supply any relevant data to you in electronic format unless you request otherwise.

It would help us to deal with your request more effectively if you would complete and return to us the attached template.

Please note that in accordance with the Data Protection Act 2018, no fee will be normally be charged for providing you with the requested information.

Kind Regards,

[Name of Principal]

## Appendix 2 - Subject Access Request (SAR) form

### SECTION 1: Details of the person completing the SAR

<b>Name</b>	
<b>Address</b>	
<b>Contact phone number</b>	
<b>E-mail address</b>	
<b>Signature</b>	

### SECTION 2: Is this SAR about you?

<input type="checkbox"/>	<b>YES:</b> I am the data subject for this SAR and I have provided my identification (see below) <b>please go to section 4</b>
<input type="checkbox"/>	<b>NO:</b> I am acting on behalf of the data subject. I have enclosed the identification for myself and the data subject (see below) <b>please go to section 3</b>

Accepted identification is anything that is issued by the government that contains a photograph, such as a passport or driving licence.

### SECTION 3: Details of the data subject

<b>Name</b>	
<b>Address</b>	
<b>Contact phone number</b>	
<b>Email address</b>	
<b>Signature</b>	

**SECTION 4: SAR information**

Please supply the detail behind the SAR and what it is you need:

Please return this form with the identification required to the Principal.

\*The information within this form will be used exclusively for the purposes of this SAR. Once the SAR has been completed your personal data will be deleted. However, we will maintain your name in our SAR register for audit purposes