

## **SUBJECT ACCESS REQUESTS**

---

The General Data Protection Regulation (GDPR) gives individuals the right to find out what information an organisation holds/stores about them. This is commonly known as a 'Subject Access Request' (SAR). This allows an individual to see what personal data an organisation holds about them, why it is held and with whom it is shared.

As a Data Controller for someone's personal data, it is your responsibility that requests for access are responded to and that the required information is provided to the requestor. This includes information that has been shared with a data processor (who processes personal data on your behalf), and they have a duty to assist you in responding. There should be a contract clause in place to ensure that they will do this.

You should record all requests and any decisions made about the response. This is especially important if you decide to restrict or refuse a request. Your decision-making needs to be clear, as it is possible that the data subject will make a complaint to the ICO about your refusal.

We strongly recommend that you maintain an SAR log so that requests can be recorded and you can demonstrate how you have been complying with them. You may still need to record more detail elsewhere and you should keep copies of all communication with the data subject. We have included a suggested SAR Log with this Bulletin.

### **Do people have to make a formal request?**

---

No. There is no particular way in which a data subject has to make a request, in respect of the exercise of any of their data protection rights. It doesn't have to be made in writing, and they don't have to specifically refer to a 'subject access request', the 'right of access' or the GDPR, to put you under a legal obligation to treat it as a valid request.

If you have implemented the model Data Protection Policy and the Privacy Notice provided by the School DPO Service, each of these provide a clear procedure for how requests may be made.

We have also created a template for a standard form (which can also help to verify the person's identity and specify what information they are looking for) but you cannot require that it be used by requestors.

### **Verifying the person's identity**

---

You should make sure that the person making the request for their data is who they say they are, to avoid disclosing someone's information to an impersonator.

You need only ask the person to prove their identity when you have doubts that they aren't who they purport to be. If the person making the request is well known to your organisation, you are not required to get formal proof of identification. For example, if

you receive a request from an email address that matches the one held on your own system, that could be relied upon as proof of identity.

If you do need to ask for confirmation of identity, do so as soon as possible. The deadline for making the full response then starts from when the person provides the necessary information.

### **What is the timeframe for responding?**

---

You have one calendar month to respond to a SAR. This will run from the day after the date the request was received or, where consent has been sought from a child of 13 or over (see below), the day after the date the consent was received.

If it is not possible to calculate the deadline because the following month is shorter, the deadline will be the last day of the following month – e.g. if a request is received on 30<sup>th</sup> May, the timeframe starts from 31<sup>st</sup> May. As there is no 31<sup>st</sup> June, the deadline to comply with the request will be 30 June. If the deadline falls on a weekend or public holiday, the deadline extends to the next working day.

The period for response may be extended by a maximum of two months where the request is considered complex. If you extend the deadline you are required to contact the individual and explain the reasons for the necessary extension.

### **Can you charge a fee?**

---

You can't charge a fee to facilitate the request, though you can charge a reasonable fee for additional copies of the information, based only on costs (e.g. for time, printing and posting).

### **Children and subject access requests**

---

Personal data about a child belongs to a 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 person should have parental responsibility for the child and clearly be asking for the information on their behalf, and 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 over**

---

Children aged 13 and above are generally regarded to have sufficient understanding to know their rights and the implications of a subject access request. Therefore, subject access requests from those with parental responsibility for pupils aged 13 and above should generally not proceed without the express permission of the pupil. In this scenario the deadline for responding to a request starts the day after the receipt of consent from the child.

In some circumstances you may determine that a child aged 13 or above does not have sufficient understanding to know what they would be consenting to, and if this is the case, then consent from the child is not required.

### **Parental requests to see the educational record for maintained schools**

---

The Education (Pupil Information) (England) Regulations 2005 give a parent their own independent right to have a copy of their child's educational record from maintained schools, and most requests to maintained schools will fall under these Regulations and not GDPR. Requests for information under these regulations should be responded to within 15 school days. A maintained school can charge for complying with such a request under these Regulations but the charge should not exceed the cost that it takes to produce it.

### **Can all the data found be provided to the Data Subject?**

---

The school must consider whether it is possible to comply with the SAR without revealing information that relates to and identifies a third party (such as another child or parent) or any other exempt information.

Where the information requested contains the personal data of a third party or parties the school should consider whether it is possible to redact the information so that this does not identify the third party or whether it is appropriate to ask for consent from the third party. Please note that references to those working in a professional capacity would not be regarded as personal information concerning them e.g. school staff members, doctors, counsellors etc.

Examples of third party information that would require special consideration:

- Safeguarding information which, if released, would put an individual at risk of significant harm
- Files containing legally privileged information
- Files containing advice from professionals such as doctors, police or probation services
- Employee references that are sent as confidential

Further advice should be sought if any information falls into the above categories.

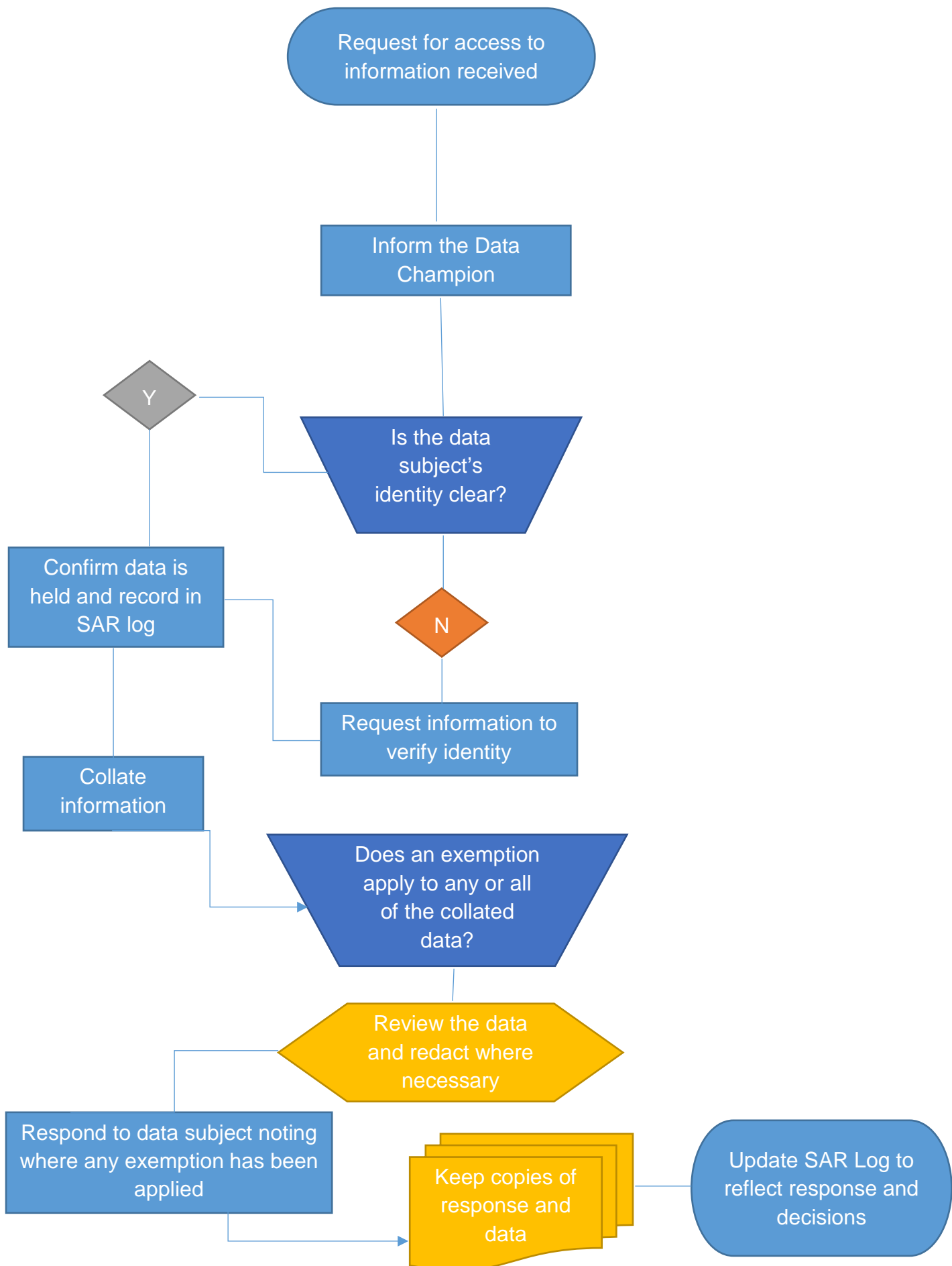
We have also included a suggested cover letter for you to use to respond to any requests including any exemptions or reasons for not processing the request.

## **Procedure for Dealing with a Subject Access Request**

---

- 1) A request for access to information is received
- 2) Inform the Data Champion (if the request is received by the DPO Service it will be forwarded on to the Data Champion).
- 3) If the request relates to a child and comes from a person with parental responsibility and the child is 13 or over and is regarded as mature enough to understand the implications of the SAR, consent should be sought from the child.
- 4) Request proof of identity from the requester if it is unclear
- 5) Confirm that the request is valid and record the request in the SAR log.
- 6) Data Champions to organise the collection of the data requested as soon as possible (it may be useful to refer to your mapping tool to determine where the information is held)
- 7) Consider whether an exemption applies to any or all of the collated data (this should be done in conjunction with the DPO Service/Legal advisers)
- 8) Review the data and redact where necessary
- 9) Respond to the data subject noting where any exemption has been applied
- 10) Keep copies of the response
- 11) Update SAR log to reflect response and decision

## SUBJECT ACCESS REQUEST PROCEDURE FLOWCHART



## SUBJECT ACCESS REQUEST FORM

By completing this form you are making a subject access request under the General Data Protection Regulation (GDPR) for personal information held about you by the Organisation that you are eligible to receive. Please complete this form and return it to .....

### The Data Subject Details

Full name of subject	
Name of school	
Relationship with the school (i.e. pupil, parent, member of staff, governor)	
Correspondence address	
Contact number and email address	
Details of the information requested	

--	--

Name:

Date: