Managing a SAR

J A Walker, Solicitor

www.jawalker.co.uk
john@jawalker.co.uk
0333 772 9763

Purpose

This guidance sets out the background to subject access requests and explains how to carry out the search and screening. Being transparent and clear about the process is critical.

When you receive a subject access request there is a statutory deadline for providing the requested information, usually one calendar month

Scope

Please search the school school/trust records for information specified in the request. One person should collate the information for the response. Make it clear to all staff who this person is.

Please keep a record of the amount of time you and your colleagues spend responding to this request.

What is personal data?

Personal data has to relate to a living individual. It identifies a person, for example by name and address. However it has to be more than that to fall within scope of a Subject Access Request.. Data can contain references to an identifiable individual, or be linked to them, but not 'relate to' them as it is not about that individual but is about another topic entirely.

An email address is personal data

The ICO give a good example.

Example Emails written by a lawyer to their client about their client's matter all contain references to the lawyer's name and place of work, which will be the lawyer's personal data. However, the content of the emails are not about the individual lawyer, but about the client's instructions.

The content of the email is not, therefore, personal data where it concerns legal advice about the client's legal query. If a complaint was then made about the lawyer's performance or advice and the emails were then used to investigate this, the legal advice given in them would become personal data.

So think carefully about what personal data really is in the context of each request.

What is a subject access request?

A subject access request can appl to all personal data held by the school/trust about a pupil. Staff member, parent/carer or other third party.

The requester may ask for all information or some.

Any student who is aged 13 (with sufficient capacity) may ask for their records.

Any person with parental responsibility or written authority can ask for records of a pupil.

HOWEVER if the pupil is over 13 (with capacity) you must consult with them before disclosing personal data.

Actions

Find relevant information

Work out where to search among your records for the requested information. Include emails and shared computer drives as well as paper records.

Based on your own knowledge decide where personal data about the individual concerned might be held, and locate that information.

You may need to search:

- **SIMS – Integris – Bromcom or similar information management systems central filing systems**
- **HR records**
- **shared drives**
- **the intranet**
- **private filing systems of particular individuals**

If necessary, you must ask colleagues to search their personal drives and email accounts, including home PCs if an individual sometimes works from home and keeps work information there.

Other locations

If you are aware of other areas in the school or trust that might also hold information about the person concerned, please arrange for these areas to be searched.

Unstructured and semi-structured data

The UK GDPR does not cover information which is not, or is not intended to be, part of a 'filing system'. However, under the Data Protection Act 2018 (DPA 2018) unstructured manual information processed only by public authorities constitutes personal data. This includes paper records that are not held as part of a filing system.

While such information is personal data under the DPA 2018, it is exempted from most of the principles and obligations in the UK GDPR and is aimed at ensuring that it is appropriately protected for requests under the Freedom of Information Act 2000.

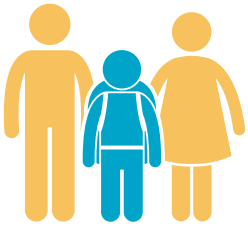
You do not have to look through unstructured personal data unless a piece of information has been specifically requested. However, you do have to look through any semi-structured data and for information held in a relevant filing system.

Legal Obligations

Section 173: Alteration etc of personal data to prevent disclosure to data subject

Section 173 relates to the processing of requests for data from individuals for their personal data. Section 173 (3) makes it a criminal offence for organisations (and persons employed by them) to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure.

Parental Disputes



It is common that school and trusts are asked to provide records when a family separates or when there are court proceedings. As the court may appoint a CAFCASS officer as part of the proceedings it is always worth being cautious about any response.

Often it is not possible to disclose a record in the case of a parental dispute without sharing information about the other party. When this

is the case, unless both disputants agree, there has to be a balance of rights. Taking advice from the DPO and also the ICO may be required in these instances.

Never simply disclose another person's information without being sure of your legal basis.

Whilst a parent has a right to information about their child, Parental Responsibility does have limits in some circumstances.

Reviewing the information

Not all personal information may be liable for disclosure. Once you have collected together the information required by the SAR, it must be considered in detail to establish if it should be disclosed.

This must be done on a case-by-case basis for each individual piece of information. In some cases you might have to disclose only parts of particular documents. There are exemptions to disclosure.

These include safeguarding information if disclosure puts another person at risk of harm, either physical or emotional. If there are pending criminal investigations or other legal proceedings disclosure may be limited or preventable. Information given in confidence also attracts a level of protection, but this has to be clear why confidentiality was in place.

Embarrassing, opinions or other information that an individual would rather not be shared does not pass the threshold to restrict release.

Support from your Data Protection Officer may be required.

How to blank out exempt and/or irrelevant information

When answering a subject access request you may have to blank out (redact) parts of a document which are not liable for disclosure, this may include details of other people, information that is not personal data but on the same page.

Hard copy documents

- **Print out the document or, if it is a paper record, make a photocopy.**
- **Using a black marker pen, blank out the exempt information.**
- **Make a photocopy of the blanked out version. This is the copy that will go to the person making the request.**

Electronic documents

- **Combine all documents into a single PDF in date sequence, using Adobe Acrobat or similar software.**
- **Using the "Redact and remove content" tool in the software to redact the exempt information by highlighting it in black.**
- **Save the blanked out version as a separate copy. This is a secure way of redacting the information, and the highlighting cannot be removed.**
- **If you are not using Adobe Acrobat, use the highlighter tool to highlight the exempt information in black.**
- **Save the blanked out version as a separate copy.**
- **Print out the document to send - do not send non-PDF documents in electronic format as it is possible the highlighting could be removed.**

Review the data before sending

Check the data subject

Check that the record is actually about the person concerned and not about someone else with the same name. Even if the document contains the correct name, check that it contains information about that person. For example, an email might carry the subject line 'Meeting about Jenny Smith but if the email only contains details about whether people can attend the meeting, the email is not about Jenny Smith.

Data Subject

You should only print out documents or emails which are about the person making the subject access request.

And remember there may be more than one person called Jenny Smith.

Screen out duplicate records

For example, if you have had an email exchange with others, you only need to print out the last email in the exchange if previous correspondence is included within it.

Obtain consent from staff acting in a private capacity

If a record was created by a member of staff acting in a private rather than an official capacity, only exceptional circumstances would justify its disclosure without their consent. If they are not prepared to disclose the record, do not disclose it.

Remove data about other individuals

You should only disclose information which is about the person making the subject access request. Where a document contains personal data about a number of individuals, including the data subject, you should not disclose the information about the third parties.

- **If the record is primarily about the data subject, with incidental information about others, you should blank out the third party information (see above).**
- **If the record is primarily about third parties, withhold it if blanking out is not possible.**
- **The school/trust must contact the third party to obtain consent to disclose the document if possible.**

The records may contain correspondence and comments about the data subject from a number of parties, including private individuals, external individuals acting in an official capacity, and school/trust staff.

In these cases we are required to balance the interests of the third party against the interests of the data subject and often blank out third party information. If this situation arises, please contact your Data Protection Officer for further guidance.

Confidential references

Do not disclose confidential references written by members of staff to bodies other than the school/trust. However, we do have to disclose references received by the school/trust.

Preventing and detecting crime

Do not disclose information which would prejudice the prevention or detection of a crime.

For example, if the police informed us that a parent or pupil is under investigation, but the person did not know this, then that information should not be provided to whilst the investigation is in progress.

However, if the investigation is closed or if the person has been informed that there is an investigation underway, then the information may be disclosed.

Legal and DPO advice

Do not disclose any records which:

- **contain advice from our lawyers or DPO**
- **contain requests for legal advice or DPO support**
- **were written as part of obtaining legal advice or DPO advice**

Negotiations

Do not disclose information which is being used, or may be used in future, in negotiations with the data subject, if the information gives away our negotiating position and disclosing the information would weaken our negotiating position.

Other exemptions

The exemptions above are those that are most likely to apply, but are not exhaustive. If you are concerned about disclosing any material, you must review this with your Data Protection Officer.

Unfavourable information

You may discover material which does not reflect favourably on you or the school/trust. For example, you may find documents which show that standard procedures have not been followed, or documents which may cause offence to the data subject. These documents must be disclosed – it is a criminal offence not to do so.

However, you should bring their contents to the attention of the relevant lead within school or the trust, and ensure that appropriate action is taken to address any issues they raise.

You must not destroy or refuse to disclose records because they would be embarrassing to disclose: this is a criminal offence if it is done after you know a subject access request has been made.

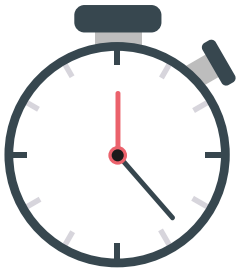
Non-compliance

There are serious consequences for the school/trust and possibly you as an individual if you do not comply with this guidance.

There are criminal sanctions if data is amended to defeat a SAR.

Time limits

The standard timescale for disclosure is one calendar month.



This can be extended by two months if the material is complex. However simply because the school is closed for holidays does not mean that an extension is automatically allowed. The ICO says that this is not exceptional.

However accessing relevant information is necessary.

If there is to be any delay, explaining this to the requester should be done at the earliest opportunity. On occasion, advice may also be required from the ICO.