Procedure

Making a Subject Access Request

Contents

1 Dealing with Subject Access Requests (SARs)

All subject access requests must be responded within **30 calendar days**. Failure to do so is a breach of the UK's General Data Protection Regulation (UK-GDPR). The 30 days should start once the person's identity has been verified. If the SAR is identified as complex, (eg, there is a high volume of data, data may be difficult to locate or there is complex redaction required), an extension of up to two months may be requested from the Data Protection Manager. This must be discussed early in the process and the data subject must be informed of any agreed extension and the reason for it within the first 30 days.

- If you receive a verbal request, you can ask for it to be put into writing but it is not a mandatory requirement. Acknowledge the request and verify their identity. Our Subject Access Request Form may be used to help support the capture of information.
- Establish what relationship the subject of the request has to Barnardo's, which team or department should be dealing with the request. Forward the request by email to the person who will be responsible for managing the SAR.
- Acknowledge receipt of the SAR and inform the person submitting the request who will be managing their request.
- A person of suitable seniority must be identified to manage the SAR; they may delegate appropriate tasks but the overall responsibility remains with

2 Dealing with Subject Access Requests (SARs) from a parent

A third-party request from a parent/guardian with legal responsibility should be verified in the same way as a self-enquiry. While this person may request access to their child's information if the child themselves is too young and/or does not have sufficient understanding, they do not have an absolute right to see the data if it is not in the child's best interest.

Before responding to a SAR for information held about a child, consider whether the child is mature enough to understand their rights.

If the parent makes the request on behalf of the child, and it is decided to respond to the child themselves, inform the parent of this and the reasons for the decision.

In **Scotland**, the law presumes that a child aged 12 years or more has the capacity to make a SAR. The presumption does not apply in **England and Wales or** in **Northern Ireland**, but it does indicate an approach that will be reasonable in many cases.

If the child can understand their rights, respond to the child rather than the parent. What matters is that the child is able to understand (in broad terms) what it means to make a SAR and how to interpret the information they receive as a result of doing so.

When deciding who to respond to consider:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

It does not follow that, just because a child has capacity to make a SAR, they also have capacity to consent to sharing their personal data with others as they may still not fully understand the implications of doing so.

3 SARs via a third party

An individual can make a subject access request via a third party.

You should ensure that the third party making the request is entitled to act on behalf of the individual. It is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney.

If it is thought that the individual may not understand what information would be disclosed to a third party who has made a SAR on their behalf, the response may be sent directly to the individual rather than to the third party. The individual may then choose to share the information with the third party after having had a chance to review it.

In some cases, an individual does not have the mental capacity to manage their own affairs. There are no specific statutory provisions enabling a third party to exercise subject access rights on such a person's behalf. But it is reasonable to assume that an attorney with authority to manage the individual's property and affairs, or a person appointed by the Court of Protection to make decisions about such matters, will have the appropriate authority. In this case the responsible Director and the Insurance section must be alerted immediately. This is not necessarily grounds for withholding the records but should be considered.

4 What to do if there's no data about the data subject

- Inform the subject that Barnardo's does not hold any information about them.
- If possible explain why there is no information, eg it has been destroyed as the retention period had been reached
- If the record is with another agency give the subject the details of who to contact to access their information.

5 Preparing the Record

Unless specific information is requested, all information held by Barnardo's about the person making the request must be collected, including electronic and paper records, photographs, video and audio recordings. This includes any emails held about the subject.

Where the request is considered excessive in nature the person responding can ask the data subject to be more specific, establishing the reason for the SAR may assist in identifying the appropriate material.

Review the records and identify any information that must be redacted, such as information about a third party. [see 10]

Identify any information that may be harmful to the subject of the data if it is shared with them. Discuss this with the DPM or DPO to decide whether there are sufficient grounds not to share the information.

6 Sharing the Record

Agree with the data subject how the data will be shared (face-to-face, email, post, etc). Ensure that the data is sent securely (encrypted e-mail, ShareFile, special delivery, etc)

Consider whether you need to talk through any of the data before it is shared, eg, could the data be harmful, does any of the data need qualifying, could it have a detrimental impact on the individual or their family. This should be discussed with Team manager/DPM when preparing the records.

If the subject identifies factual inaccuracies in core data amend the record. Personal data may not be inaccurate if it faithfully represents someone's opinion about an individual, even if the opinion proves incorrect. In these circumstances, the data would not need to

be "corrected", but a note must be added stating that the subject disagrees with the opinion.

If dissatisfied the subject may make a complaint to the Information Commissioner's Office.

7 Accessibility

If the person making the request is disabled we have a legal duty to make reasonable adjustments for them if they want to make a SAR.

If the request is complex, it would be good practice to document it in an accessible format and to send it to the disabled person to confirm the details of the request.

If necessary respond in a format that is accessible to the disabled person, such as large print, email or audio formats.

8 Recording SARs

Once the process is complete, you need to record details of the SAR and outcome on SAR log in OneTrust Guidance on how to complete the SAR log can be found here.

9 Risks of Litigation

If the subject is requesting access to their records in order to act against Barnardo's or other organisations, inform the responsible Director and the Insurance department immediately. This is not grounds to prevent the information being shared with the subject.

10 Guidance on Redaction

To redact means to remove or delete information from a record. It can be deleted electrically or it can be concealed using redaction tape, concealer fluid or a marker pen and the page photocopied. Particularly when relying on marker pen, which often does not fully conceal text even after photocopying, it is important to check the final redaction to ensure that none of the redacted information is visible.

We are required to provide the information, not the documents. If it is easier to extract the information from a document this may be done, if it is included in a report concerning a number of different people for example, but if information is being withheld about the subject this must be indicated and the document or report should include a brief note explaining the redaction.

It should be noted that, although redaction of certain information is permitted, it is not acceptable to amend or delete data where there is no reason for redacting unless the data has otherwise been amended or deleted in the ordinary course of business.

10.1 Recording redactions

A copy of the redacted record must be held on the file of the subject.

Full details of the reasons that any data is being redacted must be recorded on the case file as the subject may make a complaint to the Information Commissioner's Office and there must be evidence of the decision making process.

10.2 Information about a third party

Identify any **third party information** (ie, information about individuals other than the subject of the record) **provided by a third party** (ie, someone other than the subject of the record). In each case, consider the data subject's right of access against the third party's rights in respect of their own personal data. Where the third party's rights take precedence, you should redact unless you have their consent to provide the information or it is reasonable to not have their consent in the circumstances. Where you do decide to redact, do not indicate that this has been removed. **Third party information provided by the subject** does not need to be redacted as it is not confidential as it is already known to the subject. However, as it is not information about the subject it may be redacted if there are reasons to do so.

Identify any **information about the subject from a third party.** Unless consent has already been obtained to share the information or the subject already has access to the information, for example they have been sent copies, contact the third party and inform them of the intention to share their data and ask their views about this. If attempting to obtain consent is not reasonable or appropriate, consider whether the third party's information should be provided without consent. When making this decision, consider all relevant information, such as (i) whether Barnardo's owes any duty of confidentiality to the third party individual; (ii) whether the third party is capable of providing consent; (iii) any previous stated refusals of consent by that third party, either in respect of the information in question or with regards to similar requests; (iv) whether the information is generally known to the data subject making the request, or whether it is publicly available; (v) the importance of the information to the requesting data subject; and (vi) the nature and type of information.

If the third party does not want the data to be shared obtain the reasons for this as data may only be withheld if there are legal grounds to do so.

Relevant information about health, education or social work professionals (acting in their professional capacities) should usually be disclosed in response to a SAR.

10.3 Additional grounds for redacting data from a third party

The following may also be relied upon as relevant:

- **Confidential references:** references Barnardo's have provided in respect of the data subject are exempt from subject access if they were given in confidence and for the purposes of the data subject's education, training, employment, or the provision of a service. Please note that any confidential references you receive are not exempt from subject access per se.
- **Publicly available information:** where an enactment requires Barnardo's to make information available to the public, any personal data included the information Barnardo's is required to publish is exempt from the right to subject access.
- **Crime and taxation:** personal data is exempt from the subject access requirement to the extent it is processed for: (i) the prevention and detection of crime; (ii) the capture and prosecution of offenders; and (iii) the assessment or collection of tax or duty. Please note that this exemption applies only to the extent that complying with the subject access request would be likely to prejudice these purposes. This exemption includes any personal data that is processed for the purpose of discharging statutory functions and consists of information obtained for this purpose from a person who held it for any of the crime or taxation purposes described above, to the extent that providing subject access to the personal data would be likely to prejudice any of the crime and taxation purposes.
- **Management information:** personal data that is processed for management forecasting or management planning, to the extent that complying with the subject access request would be likely to prejudice the business or other activity of the organisation.
- **Negotiations with the requester:** personal data that consists of a record of Barnardo's intentions in negotiations with an individual is exempt from the right of subject access to the extent compliance would likely prejudice those negotiations.
- **Legal advice and proceedings:** personal data is exempt from the right of subject access where it consists of information for which legal professional privilege could be claimed in legal proceedings.

Martine King
Data Protection Officer
January 2022