THE BLUE SCHOOL

CHURCH OF ENGLAND

Whatever you do in word or deed,
do everything in the name of the Lord Jesus,
giving thanks to God the Father through him.

Colossians 3:17

Policy Subject Access Review Procedure

Author Headteacher

Ratified November 2020

Review Autumn 2022

Subject Access Request Procedure

This procedure is based on guidance on Subject Access Request(SAR) produced by the Information Commissioner's Office (ICO).

Subject Access Request Rights

Individuals have the right to obtain:

- Confirmation that their data is being processed
- A copy of their personal data.

Neither the GDPR nor the DPA 2018 specify what constitutes a valid request, therefore;

- It can be in any format, verbal or written form (Letter, email, social media).
- Does not have to include the phrase "subject access request" or "Article 15".
- Requester just needs to make it clear they want a copy of their personal data.
- Can come from a third party on behalf of the data subject.
- Can come form a joint controller or outsourced processor that you work with.

Key Principles:

- **Communicate with the requester to establish what they want, especially with "All Data Access Request"**
- **Log and document the process for posterity.**
- **Present the data as clearly as possible which shows how you have responded to the request**

Rights of Children:

Regardless of their age, an individual is in charge of their own data over anyone else, even their parent or guardian.
This has implications for both requests by, and or for a child. A child being an individual younger than the age of 18.

If you are confident that they are mature enough to understand their rights then, you should respond directly to the child.
In this case then a Parent or Guardian would need the written permission of the child to act on their behalf (see 3rd party requests).
Alternatively, if it is clearly evident that the child is not mature enough then their parents/guardians can exercise their rights on their behalf.

In Scotland if someone is aged 12 years or over, they are presumed of sufficient age and maturity, however this does not apply in England, but it is a good indicator level of what could be reasonable.
For borderline cases then you can use the following to make an assessment;

- 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.

3rd Party Requests

An individual other than the data subject can submit a SAR most commonly this is utilised by solicitors working on behalf of an individual.

These 3rd parties would need written authorisation from the individual to act on their behalf. If there are any doubts regarding their authority, then contact the data subject directly to confirm.

Full Refusal to comply with a request:

You can refuse to comply with a request in full if it is:

a) Manifestly Unfounded

- The individual clearly has no intention to exercise their right of access. For example, an individual makes a request, but then offers to withdraw it in return for some form of benefit from the organisation; or
- The request is malicious in intent and is being used to harass an organisation with no real purposes other than to cause disruption. For example:
- The individual has explicitly stated, in the request itself or in other communications, that they intend to cause disruption;
- The request makes unsubstantiated accusations against you or specific employees;
- The individual is targeting a particular employee against whom they have some personal grudge; or
- The individual systematically sends different requests to you as part of a campaign, e.g. once a week, with the intention of causing disruption.

There must be an obvious or clear quality to it being Manifestly unfounded.
You should consider if you can prove if the individual genuinely wants to exercise their rights or not.

b) Excessive.

- It repeats the substance of previous requests and a reasonable interval has not elapsed; or
- It overlaps with other requests.

However, it depends on the circumstances. It will not necessarily be excessive just because the individual:

- Requested a large amount of information, even if you might find the request burdensome. Instead you should consider asking them for more information to help you locate what they want.
- Wanted to receive a further copy of information they have requested previously. In this situation a controller can charge a reasonable fee for the administrative costs of providing this information again and it is unlikely that this would be an excessive request;
- Made an overlapping request relating to a separate set of information; or
- Previously submitted requests which have been manifestly unfounded or excessive.
- When deciding whether a reasonable interval has elapsed you should consider:
- The nature of the data – this could include whether it is particularly sensitive;
- The purposes of the processing – these could include whether the processing is likely to cause detriment (harm) to the requester if disclosed; and
- How often the data is altered – if information is unlikely to have changed between requests, you may decide you do not need to respond to the same request twice. However, if you have deleted information since the last request you should inform the individual of this.

N.B Always consider when refusing a request you have to be able to demonstrate to the individual and ICO why you have made that decision.

<u>Receiving a Subject Access Request</u>

On receipt of a confirmed or potential SAR, the staff member or data processor must immediately notify Rachel Jones at office@theblueschool.com
They will make a decision where to refer the matter to the Data Protection Officer (DPO) Mr David Coy, Data Protection Service Manager, London Diocesan Board for Schools, 36 Causton Street, London, SW1P 4AU Email: david.coy@london.anglican.org

When a SAR is received it should be immediately entered onto the Subject Access Request log and given a reference number e.g. SAR2019001, in all future communications this reference number should be used to discuss the SAR.
The Log should record the, who, when, what, and why of the process.

Additionally, a folder should be created under the reference number and all associated documentation regarding the SAR be kept in the file for posterity.

Irrespective of whether the DPO is notified or not the response to the breach will follow the same path and be

be broken down into four distinct sections: **Acknowledgment, Collection, Review, Response**

N.B No data should be deleted to preemptively prevent it from being released, this is illegal. In all likelihood it can be reviewed

Timeframe of Response

The Data Protection Act 2018 gives a timeframe of one calendar month from the date of receipt, for responding to a SAR. This is irrespective of the number of days in the month e.g. Received 17th July, Deadline 18th July.

Where this is not possible because the next month does not have a corresponding day, then the deadline is the last day of the month e.g. Received January 31st, Deadline 28th February.

Stage 1: Acknowledgment:

Sending a formal acknowledgement to confirm that:

- A SAR has been received.
- The date of receipt.
- What you believe the SAR is regarding.
- Whether anything further is needed from the Data subject i.e. clarification or refinement of the SAR, ID for verification.
- The Timeframe for a response.
- How they would like to/will receive the data i.e. paper pick up, paper posting, electronic sending.

The acknowledgement can be sent electronically or in paper format, it is not recommended that this is undertaken verbally.

Content of SAR:

It is important that you state verbatim what the individual has requested and give them the opportunity to confirm that you have understood the request correctly. This will save wasted time collecting data which is not required.

Clarification or Refinement:

If a request is received with asks for “All Data”, it is highly recommended that you seek further refinement to allow you to efficiently respond to the request within the timeframe.

ID Verification:

It is important that you are satisfied that the request is genuine, and the individual is who they say they are. You don’t want to release information to an incorrect recipient. Therefore, if you are unsure, request a copy of photo ID to confirm the identity of the requester.

Timeframe for Response:
Although the official process stated that there is a timeframe of one calendar month from the day after receipt.
This can be delayed or extended.
If you have requested further clarification or ID verification, the clock does not start until this is received. This should be explained in your acknowledgment.
If you believe you cannot respond within the one calendar month timeframe, then you can extend the deadline for up to two months. Most commonly this extension is used if the request is complex or extensive, “All Data” requests commonly fall into this category. Hence refining the “All Data” request is beneficial for both the requester and the school.

Stage 2 Collection:
This is where the data that has been requested is collated and stored ready for review, this can be done in either an electronic or paper format. Which is more efficient will vary depending on what has been requested and how it has been requested. i.e. what format the original copy of the data is in and how it is to be sent.

Using the confirmed requested content of the SAR, you should work down the list and point for point to collect the data.

It is recommended that someone who has an appropriate level of authority is selected to collect the data requested.

Record of Data Processing:
This can be used as an assistance tool to

a) Understand what data is being held on individuals
b) Where it is being held; Management software, filing cabinets.
c) What outsourced processors need to be contacted.

Contacting Outsourced processors.
If some of the requested data is being held by an outsourced processor, then they would need to be contacted to inform them of the SAR and that their assistance is needed.
If they are a Joint controller i.e. Local Council, Social services, it may be applicable to inform them that you have had a SAR and they may expect one shortly as well, as you cannot make the decision yourself to release the data.

Collection of Emails:
If the request involves emails and their contents i.e. all emails which contain my name Jo Bloggs.
Then you will need to either

a) Contact all staff to ask for them to forward these emails.
b) Use IT support to run a mass email search remotely.

In either case, it is often a good idea to advise staff before, then they can preemptively contact you if they think the emails may present a problem.
If staff are forwarding emails to then up an email account like SAR@School.uk and ask for all emails to be sent to their work rather than a personal account, where they could become mixed up with regular incoming communications.
N.B. During the Collection and Review stages it can help that data is grouped together which respond to specific aspects of the request or which form narratives. E.g. all internal emails, Pupil file, exam results.

Stage 3 Review:

It is recommended this part of the process is undertaken by the Headteacher and or DPO as this is where the collected data is reviewed, and items are removed or redacted. Therefore, the person making the decision should have the executive authority to do so.
The DPA 2018 states you need not have to comply with a request in full or aspects if it would mean disclosing information about another individual who can be identified from that information, except if:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

Items would include:

- Names of other data subjects
- Email addresses of other Data subjects
- Data relating to other Data Subjects i.e. where the individual forms part of a bigger data set; exam results, class lists.
- Items which could cause emotional or physical harm or distress to the data subject or other data subjects.

This is not an exhaustive list and it is very much a case by case basis of what could and should be released. This should not be done remotely without seeing the item.
It is worth noting that anything which is removed needs to be justified in the response.
In addition, if names and emails are redacted for one individual because consent is not given and others are, this may create a disparity which will need explaining.

How the redaction occurs is dependent on the format it is presented in, paper redaction can be done by marker pen, tippex and then photocopying.
If the items are in an electronic format then you can highlight in black and print them out or use the Acrobat Reader Pro, redaction function.
Please note, if you are sending the information electronically, then don't redact the document in a way that can be reversed.

A copy of both what is and what is not supplied in the response should be kept in the file for posterity.

Stage 4: Response.

This is where in a formal correspondence you explain the process and result of the collection and review process to the data subject and present them with the information. It should include:

- What and where was searched to comply with the request, e.g. paper records, SIMS, emails, CPOMS
- Reconfirm what was asked for
- What is being supplied
- What is not being supplied and why.
- Why items have been redacted e.g. removing any information which would identify any data subjects other than themselves
- Ability to discuss this further with the school.
- Right to refer to the ICO and contact details.

N.B. When supplying the data, it must be in an understandable format. Therefore, it is recommended to explain what is what and why. Go point for point with what was requested and what has and has not been supplied.
Label what the individual items are so a layman could understand it.