



Bishop Wilkinson
Catholic Education Trust
Through Christ, in Partnership

Data Subject Access Request Policy

Date Approved by Trust	July 2026
Statutory Policy	No
Required on Website	No
Review Period	2 Years
Next Review Date	July 2028
Reviewed by	DPO

1. Revision History

The below table provides the revision history for this document. Each revision has an associated date, issue number, and description of the changes and/or content. The document revisions appear in descending order, with the most-recent iteration appearing first in the table.

Date	Version	Description	Author
29/06/2026	0.f	4 th Review, changes to reflect current procedures and update legislation	Sarah Burns Data2Action
30/05/2024	0.e	3 rd Review, no changes	Sarah Burns Data2Action
03/07/2023	0.d	2 nd Review changes to reflect procedural changes with introduction of VDPO	Sarah Burns, Data2Action
15/07/2022	0.c	1 st Review no changes	Sarah Burns, Data2Action
09/06/2021	0.b	Final Version	Sarah Burns, Data2Action
18/05/2021	0.a	Initial Draft	Karen Latimer Data2Action

2. Document Approval

Document Name	Data Subject Access Request Process
Publication Date	July 2026
Prepared by	Sarah Burns, Data2Action
Approval (Name & Organization)	BWCET Directors

3. Background

This document sets out the requirements and process for identifying and managing a Data Subject Access Request (SAR) within Bishop Wilkinson Catholic Education Trust (the Trust).

Under data protection legislation, individuals have the right to:

- request access to their personal data
- receive a copy of their personal data (subject to lawful exemptions)
- understand how their personal data is used

The Trust has a legal responsibility to identify that an individual has made a request and handle it accordingly.

This document is for information and use by all employees of the Trust, any associates, contractors or agency staff and third-party processors and describes what a subject access request is, how to identify it, and what to do next in logging it and responding to it.

Associated documents: Bishop Wilkinson Catholic Education Trust Data Subject Access Request Form (Appendix A) is stored on our internal server and can be accessed upon request.

4. What is a data Subject Access Request?

An individual can make a subject access request to anyone in the Trust either verbally or in writing. The request does not have to be to a specific person or contact point and does not specifically have to include the phrase 'subject access request'. Providing the individual is asking for records of their own personal data, then it must be treated as a SAR.

There are two distinct rights to information the Trust holds:

1. A pupil's, parent's or staff members right of access to their own personal data under article 15 of the UK GDPR.

Individuals are only entitled to receive information that relates to or is about them, however they may ask someone else to exercise their right and act on their behalf.

Where a legitimate request is made, the Trust will provide a response without undue delay and no later than within one calendar month, although this can be extended by a further two months in certain circumstances.

2. A parent's right to access their child's education record (e.g. attendance records, behaviour records, termly/ annual school reports, letters to parents from school about their child etc) under the Education (Pupil Information) Regulations 2005.

In England, this right only applies to maintained schools therefore Academies/ Trusts are under no obligation to provide this information. Should we agree to provide this, we will do so within 15 working school days.

The rights children have to make a request

Children can make their own Subject Access Request, regardless of age.

Parents/carers may submit a SAR on behalf of their child only where the child is not able to exercise their own rights, or where they ask them to act on their behalf.

Where this is the case the Trust:

- may ask for written confirmation (consent) from the child. We will first assess whether requesting consent is in the best interests of the child and whether they are able to understand the request.
- will always consider whether responding to the parent's request is in the best interests of the child.

Generally, in England, children over the age of 12 are considered sufficiently competent to exercise their own rights, however each request will be considered on a case by case basis.

Where consent to proceed is deemed appropriate, the time period to respond is paused until we receive the outstanding information.

5. Confirming Identification of Requester

Immediately upon receipt of a data subject access request, check with the requester that you have understood their request and check their identity to ensure they are in fact who they say they are. This is important as only personal data relating to the data subject must be issued either to the data subject or an authorised third party (i.e. parent). An individual's ID can be checked via internal systems such as match names, parental responsibility, email address and contact details within Arbor. If internal checks do not adequately verify an individual, then you should seek this from the requester. Where this is the case, the timeframe to respond is paused until the ID is verified.

On occasion, you may need to seek clarity as to the specific nature of the request. Where this is the case, the request is again paused until clarity is provided.

Requests must not be routinely paused and can only be done where there are legitimate reasons to do so.

Report the request to the Headteacher/DPO for further assessment. Any additional information or evidence required to confirm identity must be sought and recorded.

All requests must be logged on the Virtual Data Protection Officer Portal (VDPO), the Headteacher with support from the DPO, should manage the request thereafter as per the requirements detailed in the next steps of this process.

6. What is an individual (data subject) entitled to?

Individuals have the right to obtain the following from the School/ Trust:

- confirmation that the School/Trust are processing their personal data
- a copy of their personal data
- other supplementary information as detailed in the Trust's Privacy Notice:
 - the purposes of our processing;
 - the categories of personal data concerned;
 - the recipients or categories of recipient we disclose the personal data to;
 - our retention period for storing the personal data
 - the existence of their right to request rectification, erasure or restriction or to object to such processing;
 - the right to lodge a complaint with the ICO or another supervisory authority;
 - information about the source of the data, where it was not obtained directly from the individual;
 - the existence of automated decision-making (including profiling); and
 - the safeguards we provide if we transfer personal data to a third country or international organisation.

As the above information is detailed in the applicable Trust Privacy Notice, as copy must be provided as part of the final response.

7. Responding to a SAR

What data to provide:

An individual is only entitled to sight of and access to their own personal data, and not to information relating to other people (unless the information is also about them, or they are acting on behalf of someone).

It is important to establish whether the information requested falls within the definition of personal data. This is where the data is about or relates to an identifiable person. To determine this, the purpose/ use of the personal information, the context and the content of the record should be carefully assessed.

Records of Processing (RoP) detail the types of personal data collected and processed by schools/Trust, how this is managed and where the data is stored and processed. A copy of the RoP is stored centrally by the DPO and should be referred to check all records of personal data are included in the response.

Typically, records held by Schools/ the Trust will include:

- Admissions records
- Attendance registers
- Pupil Profile Summary from Arbor
- Attainment and progress results
- Annual school reports
- Behaviour/ achievement records
- Curriculum records
- SEND records
- Safeguarding records (i.e held in CPOMs)
- Medical records
- School trips
- Photographs
- CCTV footage
- Staff records (name, address, DoB, next of kins, employment contract, payroll information, attendance records, requests for leave, appraisals, disciplinary records etc)

How to provide copies of the personal data:

If an individual makes a request electronically, the school/Trust should provide the information in a commonly used electronic format, unless the individual requests otherwise. The Trust must use a secure means by which the documents are encrypted and therefore only accessed in a readable format by the recipient.

Individuals should be given every opportunity to access/ collect the records once they've been prepared for disclosure. On occasions, individuals may delay access/ collection therefore they should be reminded once with all records made available for up to a six month period.

All records relating to the SAR should be retained for 12 months after the SAR has been closed.

Can we amend the data before we send it?

A SAR relates to the data held at the time the request is received. The ICO does acknowledge however that *'in many cases, routine use of the data may result in it being amended or even deleted while you are dealing with the request. So, it would be reasonable for you to supply information you hold when you send out a response, even if this is different to that held when you received the request'*.

It would not however be acceptable to amend or delete the data if it would not otherwise have been amended. Under the Data Protection Act 2018 (DPA 2018), it is an offence to make any amendment with the intention of preventing its disclosure.

Can we charge a fee?

The school/Trust should not **normally** charge a fee for managing a subject access request. This may however be considered, and where only agreed by a Trust Director, where the administrative costs of complying with the request are:

- manifestly unfounded or excessive
- an individual requests further copies of their data following a request.

Where a fee is necessary, complying with the SAR will not commence until the fee is received. Alternatively, the Trust may refuse to comply with a request which is manifestly unfounded or excessive, see Section 9.

How long do we have to comply with a SAR?

The SAR must be complied without undue delay and at the latest within **one month** of receipt of the request or (if later) within one month of receipt of:

- any requested information to clarify the request
- any information requested to confirm the requester's identity
- a fee (only in certain circumstances)

The one-month timeframe should be calculated from the day it is received (whether it is a working day or not) until the corresponding calendar date in the next month. If this date falls on a weekend or Bank Holiday, then it should be provided on the next working day.

In exceptional circumstances, the timeframe may be extended up to a period of two further months. This is only where the request is deemed to be complex and where the DPO has been consulted.

8. Subject Access Request Log

All relevant information must be recorded on the VDPO.

The following checklist should be used to ensure all relevant information has been provided back to the data subject;

- Have you identified and included all the personal data for the data subject?
- The SAR does not include any personal data about another data subject
- Have you advised of the 'purpose of the processing activity' undertaken?
- Have you advised of the categories of personal data processed?
- Have you advised who else we disclose personal data to?
- Have you advised how long the retention periods are?
- Have you reminded the data subject of their rights?
- Have you reminded them of their right to complain to the ICO?
- Have you advised them of any 'Automated Decision Making' or 'Profiling' activity?

- Have you advised them of safeguards in place when transferring data to third countries?
- Have you reminded them of the Privacy Notice?
- Has the information been adequately secured before sending it to the data subject?
- If the request is made electronically, has the response been issued in a commonly used electronic format?
- Have you responded within 1 month? If not, are we advising the data subject and offering the ICO details?

Remember: You may refuse a SAR **only** in a few exceptional circumstances but you must refer to the DPO where this is to be considered.

These instances may include if the request is manifestly unfounded or excessive e.g.

- The individual has no intention on exercising their rights and offers to withdraw for some form of benefit
- If the individual has advised they are requesting this to cause disruption
- If the individual is targeting employees or the Trust with unsubstantiated accusations or a grudge
- If the Trust receives differing requests as part of a campaign to disrupt
- If rejected - please refer to the DPO immediately

For further information please refer to the Headteacher/DPO/Director of Governance or a member of your SLT.

9. Supporting Documentation

- Appendix A – Subject Access Request Form (see website)