



Data Subject Access Request Policy

Date Approved by School	Sep 25
Statutory Policy	No
Required on Website	No
Review Period	2 Years
Next Review Date	Sep 27
Reviewed by	DPO

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
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

1. Document Approval

Document Name	Data Subject Access Request Process
Publication Date	July 2024
Prepared by	Sarah Burns, Data2Action
Approval (Name & Organization)	C. Spencer Highfield Community Primary School

2. Background

This document sets out the requirements and process for identifying and managing a Data Subject Access Request (SAR) within Highfield Community Primary School (the School).

There are two ways to accessing pupil information:

- Under Data Protection legislation, the UK GDPR grants the right of access to pupils and those with parental responsibility. In the UK, parents or those with parental rights have the right to access their child's data where they are 12 years or younger. When a child reaches 13 years of age, they are deemed sufficiently literate to understand what they are requesting under a SAR. Parents or those with parental rights of children 13 years or older therefore cannot request a SAR without their child's consent, unless the child is not deemed sufficiently capable of understanding the request.
- Under the education regulations, those with parental responsibility have the right to view their child's education record. The timescale to provide a child's education record under the education regulation is 15 days and therefore is different to a SAR under Data Protection Regulation which is 1 month. Its therefore vital to clarify the request and determine under which regulation the request applies.

3. Introduction

The UK GDPR gives data subjects the right to obtain a copy of their personal data as well as other supplementary information. This is also known as the 'right to access' and helps individuals to understand how and why an organisation is using their data, and check they are doing it lawfully.

The School 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 School, 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: Highfield Community Primary School 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 School 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.

If possible, should a data subject access request be received within a school, the School GDPR Data Subject Access Request Form should be forwarded to the requester in the first instance for completion of all required information and obtain necessary consent.

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).

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:

- confirmation that the School are processing their personal data
- a copy of their personal data
- other supplementary information as detailed in the School'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.

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). Therefore, it is important to establish whether the information requested falls within the definition of personal data.

Records of Processing (RoP) detail the types of personal data collected and processed by schools, 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.

How to provide copies of the personal data:

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

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 should not charge a fee for managing a subject access request. This may however be considered, and where only agreed by a Headteacher, 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 School 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.

If the required one-month response timescale is not achievable for example, if the school are collating several requests, extra time is acceptable up to a maximum extra two months however, the data subject should be advised of the situation within one month of receiving the request outlining why more time is needed.

8. Subject Access Request Log

All relevant information should 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 in a few exceptional circumstances but please refer to the DPO in every instance.

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 School with unsubstantiated accusations or a grudge
- If the School 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