Academies Trust

8th Floor, Angel Square,
Manchester, M60 0AG

Subject Access Request (SAR) Procedure

Appendix 4 of the Data Protection Policy

Approved by the Trust Board's Audit and Risk Committee on 2 October 2025

Applicable from 3 October 2025

Last Reviewed:	August 2025 (in preparation to seek approval in October 2025)
Reviewed by:	Tammy Pyszky, Head of Data Protection
Next Review Date:	October 2026
Version Changes:	Amended to explain acronyms previously used.

	Amended to identify the role of data protection ambassadors in dealing with requests.

This document will be reviewed annually and more frequently when significant changes are made to the law.

Contents

Appendix 4: Subject Access Request (SAR) Procedure

A4.1 Introduction

We process personal data in line with all of the legal rights of data subjects, including their right to:

- Be informed about their data being processed, which links to the first Data Protection Principle of fair, lawful and transparent processing;
- Request access to their data that we hold;
- Ask for inaccurate data to be rectified;
- Ask for data to be erased (sometimes known as the "right to be forgotten");
- Restrict processing of their data, in limited circumstances;
- Object to the processing, in some circumstances, including stopping their data being used for direct marketing;
- Data portability, which means to receive copies of some of their data in a format that can be easily used by another organisation or person;
- Not be subject to automated decision making or profiling, if it has legal effects or similarly significant effects on the data subjects;
- Withdraw consent when we are relying on consent to process their data;
- Make a complaint to the Information Commissioner's Office (ICO) or seek to enforce their rights through the courts.

This procedure supports our Data Protection Policy, and explains how we respond to requests from, or on behalf of, individuals for access to the data we hold that is about the individual. This is known as the right to access, and is a legal right under the UK GDPR and the Data Protection Act (DPA) 2018. Requests are known as Subject Access Requests, or SARs.

In addition, pupils, or parents on their behalf, who attend one of our special schools, have the right to access the pupil's curricular and educational records, under the Education (Pupil Information) (England) Regulations 2005 (EPIR 2005). This legal obligation applies only to our special academies, and is not a legal requirement for other academies.

For any queries about how to exercise any of the rights above, contact the relevant academy's data protection ambassador or our Head of Data Protection.

A4.2 Scope and Responsibilities

The right to access applies to all pupils, parents, staff and anyone else that we hold personal data about. In some circumstances, for example with pupils, a parent or other person with authority may make the Subject Access Request on their behalf.

All leaders are responsible for ensuring their staff read and understand this procedure as they may receive a SAR on behalf of their academy.

SARs received by an individual academy should be passed to the academy's data protection ambassador for them to respond. SARs received by a member of the Central Team will be passed to the Head of Data Protection.

Our Head of Data Protection provides assistance and further guidance on responding to SARs. Further guidance is also available in the Data Protection and Information Governance Handbook available via the ambassadors' toolkit.

Any individual who purposefully alters, defaces, blocks, erases, destroys or conceals information to prevent it being provided to a data subject who has requested it, and has a right to receive it, may be committing an offence.

A4.3 Receiving a valid SAR

Format: A SAR does not need to be in writing, it can be in any format, including a letter, email, text message, over social media, over the telephone, or face to face, and can be made to any representative of our academies.

Content: A SAR does not need to refer to data protection legislation or be described as a subject access request to be a valid SAR. Any request for access to personal information from, or on behalf of, a data subject, should be treated as a SAR.

Identity and Authority: We must verify the identity of the person making the SAR, and if the SAR is being made on behalf of someone else, we must confirm they have authority to act on their behalf in exercising their rights. Checking identity should not be used as a delaying tactic, and how to verify identity will depend on who is making the SAR, and how well they are known to the person handling the request. For example, a staff member will not usually be required to confirm their identity, but a request from a former staff member, or on behalf of someone else, may need to be verified.

A parent / person with parental responsibility does not automatically have the right to make a SAR on behalf of their child.

A child may exercise these rights on their own behalf if we believe they are competent to do so. Assessing competence is based on the age, maturity and level of understanding of the child. Each situation will be decided in collaboration with the professionals working with the child, but 12 years is regarded as a starting point. A child should not be considered competent if it is evident that he or she is acting against their own best interests or under pressure from a parent or other person with authority.

Where a SAR is received from a parent of a competent child, consent to process the request and release all/part of the information will be sought from the child.

No charge: In most cases, a SAR will be responded to free of charge. In limited circumstances, where a request is manifestly unfounded or excessive an appropriate charge may be made.

Requests made under EPIR 2005 may be charged for. A proposed charge should be agreed with the Headteacher.

Refusing to fulfil a SAR: In limited circumstances, the request or elements of it may be refused under the exemptions in the DPA 2018, for example:

- if the requestor cannot confirm their identity or authority to make the request on behalf of another person, the request will be refused until confirmation is provided;
- where a request is manifestly unfounded or manifestly excessive;
- information relating to education data, social work data or health data if it might cause serious harm to the physical or mental health of the data subject or another individual (this applies even when a competent child has consented to their parent receiving their data).

Elements of data held that may be withheld or redacted, include:

- information that would reveal that a child is at risk of abuse, where disclosure of that information would not be in the child's best interests (this applies even when a competent child has consented to their parent receiving their data);
- information contained in adoption and parental order records;
- certain information given to a court in proceedings concerning a child.

A4.4 Responding to a SAR

Timescales: SARs must be responded to as soon as possible, and within one month at the latest.

In the case of complex or multiple requests an extension of up to an extra two months can be applied, in consultation with the Head of Data Protection, but the requestor must be informed of the extension within the first month.

The calculation of time will commence once the SAR is determined as valid.

An acknowledgement should be sent to the requestor as soon as possible to inform them that the SAR has been received, the start date, and that it is being processed.

For SARs, school holidays, bank holidays and weekends are all included within the month. For example, a valid SAR received on 20th July should be fulfilled by 20th August despite the school closure.

Requests made under EPIR 2005 must be fulfilled within 15 school days - this applies to our special schools only and is not applicable to our other academies.

Format: The colleague dealing with the request will decide with the requestor, the most appropriate and preferred method of providing information. Usually this is via a Google Drive link, but may be by other means if requested by the requestor.

Content: The 'right to access' allows the requestor to receive information held about them, as a data subject. The requestor will not necessarily receive every version of information, if it is held in different ways or duplicated. Access is to the data, not the particular documents.

Third party data: Where the person's data is combined with another person's data, which does or could identify that other person (third party), that data may be redacted, or withheld if redaction would not fully prevent the other person being identified. Data can be disclosed that identifies the third party if that person has given their consent to disclose it, or it is judged to be reasonable to disclose the information without that person's consent. Deciding if it is reasonable should take into account things such as the type of information, any duty of confidentiality owed, the role of the other person, whether the person is capable of giving consent, and whether they have expressly refused consent.

A4.5 Exemptions

Exemptions under the DPA 2018 allow us to withhold data from a SAR in some further circumstances, including amongst others:

- where legal professional privilege applies;
- where management forecasts or negotiations could be prejudiced by disclosing the data;
- confidential references; and
- where exam results are requested but they are not yet due to be published.

Colleagues should seek advice from the Head of Data Protection in regard to the application of exemptions. If in doubt do not disclose information, as it can always be disclosed at a later date.

Response: When sending the relevant data to the requestor, the information should be clear, so any codes or jargon used should be explained in the SAR response. In responding to requests we also explain to data subjects they have the right to make a complaint to the ICO or seek to enforce their rights through the courts.

Data subjects also have a right to receive, in response to their SAR, the following information, which is contained within our Privacy Notice (a link to which will accompany the release):

- the purposes of our processing;
- the categories of personal data concerned;
- the recipients or categories of recipient we disclose the personal data to;
- retention periods for storing the personal data or, where this is not possible, our criteria for determining how long it will be stored for;
- the existence of their right to request rectification, erasure or restriction or to object to such processing;

- information about the source of the data, where it was not obtained directly from the individual;
- the existence of any automated decision-making (including profiling); and
- the safeguards we provide if we transfer their personal data to a third country or international organisation.

Record Keeping: The receipt of SARs and all decisions made will be logged using the Trust's chosen data protection platform, GDPRiS. This ensures timescales are being met and SARs are being handled appropriately.