OUR LADY OF LOURDES

CATHOLIC MULTI-ACADEMY TRUST

Policy Procedure for Receiving and Responding to Subject Access Requests

May 2026

Nottingham Diocese Multi Academy Trusts

CATHOLIC SCHOOLS Moving Forward Together

Title of policy:	Subject Access Request Policy
Author and policy owner in the Executive Team:	Tamer Robson, DPO
Reviewer:	Tamer Robson, DPO Audit & Risk Committee OLoL Trust Board
Normal review frequency:	Two years
Version number:	1.3
Committee approval date:	13 May 2026
Trust Board approval date:	20 May 2026
Date of next review:	01 May 2028

Document review and editorial updates:

Version control	Date	Reason for Revision	Key revisions included
1.1	04/02/2025	Exceptional Review	Updated for administrative fee for Subject Access Requests
1.2	01/02/2026	Exceptional Review	Updated in line with DUAA update to GDPR
1.3	06/05/2026	Exceptional Review	Refers to new Data Protection Complaints Policy
Choose an item.	Click or tap to enter a date.	Choose an item.	
Choose an item.	Click or tap to enter a date.	Choose an item.	
Choose an item.	Click or tap to enter a date.	Choose an item.	

Contents

1	Policy statement	**4**
2	Definition of data protection terms	**4**
3	Recognising a subject access request	**4**
4	Verifying the identity of a Requester	**4**
5	Reasonable and Proportionate Searches	**5**
6	Fee for Responding to Requests	**5**
7	Time Period for Responding to a SAR	**5**
8	Form of Response	**6**
9	Sharing Information with Third Parties	**6**
10	Withholding Information	**7**
11	Process for dealing with a Subject Access Request	**8**
12	Data Protection Complaints	**8**
12	Annex 1 – Definitions	**10**
13	Annex 2 – SAR Acknowledgement Letter	**11**
14	Annex 3 – SAR Response Template	**12**
15	Annex 4 – Fees Table for Administrative Cost of Excessive SAR	**15**

1. Policy Statement

1.1. All **Data Subjects** have rights of access to their **personal data**. This document sets out the procedure to be followed in relation to any requests made for the disclosure of **personal data processed** by the Trust/School.

2. Definition of data protection terms

2.1. All defined terms in this policy are indicated in bold text, and a list of definitions is included in Annex 1 to this policy.

3. Recognising a subject access request

3.1. As the Trust/School **processes personal data** concerning **data subjects**, those **data subjects** have the right to access that **personal data** under Data Protection law. A request to access this personal data is known as a subject access request or SAR.

3.2. A **data subject** is generally only entitled to access their own **personal data**, and not to information relating to other people.

3.3. Any request by a **data subject** for access to their **personal data** is a SAR. This includes requests received in writing, by email, and verbally.

3.4. If any member of our **Workforce** receives a request for information, they should inform the Trust's Data Protection Officer ("DPO") as soon as possible.

3.5. In order that the Trust/School is properly able to understand the nature of any SAR and to verify the identity of the requester, <u>any requester making a request verbally should be asked to put their request in writing and direct this to the Trust DPO</u>.

3.6. A SAR will be considered and responded to in accordance with the Data Protection Law.

3.7. Any SAR must be notified to the DPO at the earliest opportunity.

4. Verifying the identity of a Requester

4.1. The Trust/School is entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are.

4.2. Where the Trust/School has reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of two or more of the following:

4.2.1. Current passport
4.2.2. Current driving licence
4.2.3. Recent utility bills with current address
4.2.4. Birth/marriage certificate
4.2.5. P45/P60
4.2.6. Recent credit card or mortgage statement

4.3. If the Trust/School is not satisfied as to the identity of the requester then the request will not be complied with, so as to avoid the potential for an inadvertent disclosure of **personal data** resulting to a data breach.

4.4. The timeline for responding to the SAR does not start until ID has been provided.

5. Reasonable and Proportionate Searches

5.1. For all SARs, a reasonable and proportionate search will be carried out on a case-by-case basis, this will usually include searching the school MIS system, Safeguarding system and the pupil file. It is not reasonable to search all emails as relevant emails will have been recorded in the MIS system, Safeguarding system or pupil file. It is not reasonable and proportionate to search all CCTV. The DPO or school GDPR Lead may seek clarification to narrow the scope of the request and the clock stops until clarification is received. A two week window may be provided to provide clarification, and if not provided within this timeframe, the request may be deemed to be closed.

6. Fee for Responding to Manifestly Unfounded or Excessive Requests

6.1. The Trust/School will usually deal with a SAR free of charge.

6.2. Where a request is considered to be manifestly unfounded or excessive a fee may be requested to cover the administrative costs of the SAR. The fee will be calculated as soon as possible and within one month of the SAR request. The timeline to respond to the SAR will commence once the administrative fees have been paid. If payment is not received for the administrative costs of the SAR within one month of being provided, the SAR request will be deemed to be closed. A fees table can be found in Annex 6. Alternatively, the Trust/School may refuse to respond to the request. If a request is considered to be manifestly unfounded or unreasonable the Trust/School will inform the requester why this is considered to be the case. The Trust DPO will consider the context of each request to determine if it is excessive.

6.3. A fee may also be requested in relation to repeat requests for copies of the same information. In these circumstances a reasonable fee will be charged taking into account the administrative costs of providing the information.

7. Time Period for Responding to a SAR

7.1. The Trust/School has one month to respond to a SAR. This will run from the later of a) the date of the request, b) the date when any additional identification (or other) information requested is received including clarification of the request, or c) payment of any required fee.

7.2. In circumstances where the Trust/School is in any reasonable doubt as to the identity of the requester, this period will not commence unless and until sufficient information has been provided by the requester as to their identity, and in the case of a third party requester the written authorisation and two forms of ID of the **data subject** has been received (see below in relation to sharing information with third parties).

7.3. The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request and may include sensitive Safeguarding data. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.

7.4. Where a request is considered to be sufficiently complex as to require an extension of the period for response, the Trust/School will notify the requester within one calendar month of receiving the request, together with reasons as to why this is considered necessary.

7.5. Subject Access Requests received towards the end of term or during periods of school closure will be deemed to be complex due to the limited resource in school and the timeline may be extended by up to two further months.

8. Form of Response

8.1. **A requester can request a response in a particular format.** In particular where a request is made by electronic means then, unless the requester has stated otherwise, the information should be provided in a commonly readable format.

9. Sharing Information with Third Parties

9.1. **Data subjects** can ask that you share their **personal data** with another person such as an appointed representative (in such cases you should request written authorisation signed by the **data subject** confirming which of their **personal data** they would like you to share with the other person). Two forms of ID are required from the data subject or their parent. E.g. if a request is received for a parent's data via a solicitor, we must receive written consent and two forms of ID from the parent before information is shared, in order to verify the request. If ID and consent are not received within two weeks, the request will be deemed to be closed.

9.2. Equally if a request is made by a person seeking the **personal data** of a **data subject**, and which purports to be made on behalf of that **data subject**, then a response must not be provided unless and until written authorisation has been provided by the **data subject**. The Trust/School should not approach the **data subject** directly but should inform the requester that it cannot respond without the written authorisation of the **data subject**.

9.3. If the Trust/School is in any doubt or has any concerns as to providing the **personal data** of the **data subject** to the third party, then it should provide the information requested directly to the **data subject**. It is then a matter for the **data subject** to decide whether to share this information with any third party.

9.4. **Personal data** belongs to the **data subject**, and in the case of the **personal data** of a child regardless of their age the rights in relation to that **personal data** are theirs and not those of their parents. Parents, in most cases, do not have automatic rights to the **personal data** of their child.

9.5. However there are circumstances where a parent can request the **personal data** of their child without requiring the consent of the child. This will depend on the maturity of the child and whether the Trust/School is confident that the child can understand their rights. Generally where a child is under 13 years of age they are deemed not to be sufficiently mature as to understand their rights of access and a parent can request access to their **personal data** on their behalf.

9.6. In relation to a child 13 years of age or older, then provided that the Trust/School is confident that they understand their rights, and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the Trust/School will require the written authorisation of the child before responding to the requester, or provide the **personal data** directly to the child in accordance with the process above.

9.7. In all cases the Trust/School should consider the particular circumstances of the case, and the above are guidelines only.

10. Withholding Information

10.1. There are circumstances where information can be withheld pursuant to a SAR. These are specific exemptions and requests should be considered on a case by case basis.

10.2. Where the information sought contains the **personal data** of third party **data subjects** then the Trust/School will:

10.2.1. Consider whether it is possible to redact information so that this does not identify those third parties, taking into account that it may be possible to identify third parties from remaining information;

10.2.2. If this is not possible, consider whether the consent of those third parties can be obtained; and

10.2.3. If consent has been refused, or it is not considered appropriate to seek that consent, then to consider whether it would be reasonable in the circumstances to disclose the information relating to those third parties. If it is not then the information may be withheld.

10.3. So far as possible, the Trust/School will inform the requester of the reasons why any information has been withheld.

10.4. Where providing a copy of the information requested would involve disproportionate effort the Trust/School will inform the requester, advising whether it would be possible for them to view the documents at the Trust/School or seeking further detail from the requester as to what they are seeking, for example key word searches that could be conducted, to identify the information that is sought.

10.5. In certain circumstances information can be withheld from the requester, including a **data subject**, on the basis that it would cause serious harm to the **data subject** or another individual. If there are any concerns in this regard, then the DPO should be consulted.

10.6. If an exemption from the right of access applies, information may be withheld e.g. the crime and taxation exemption, or child abuse data to the extent that complying with the request would not be in the best interests of the child.

11. Process for dealing with a Subject Access Request

11.1. When a subject access request is received, the Trust/School will:

11.1.1. immediately notify the Trust's DPO who will, together with the School's GDPR Lead, be responsible for managing the response

11.1.2. take all reasonable and proportionate steps to identify and disclose the data relating to the request;

11.1.3. never delete information relating to a subject access request, unless it would have been deleted in the ordinary course of events – it is an offence to amend or delete data following receipt of a SAR that would not have otherwise been so amended or deleted;

11.1.4. consider whether to seek consent from any third parties which might be identifiable from the data being disclosed;

11.1.5. seek legal advice, where necessary, to determine whether the Trust/School is required to comply with the request or supply the information sought;

11.1.6. provide a written response, including an explanation of the types of data provided and whether and as far as possible for what reasons any data has been withheld (see template at Annex 3,4,5); and

11.1.7. ensure that information disclosed is clear and technical terms are clarified and explained.

12. Data Protection Complaints

12.1. Any complaints relating to the processing of personal data covered by this policy should be made in accordance with the Data Protection Complaints Policy.
If following internal review, the individual remains dissatisfied, they have the right to complain to the Information Commissioner, who oversees compliance with data protection law. Individuals should write to: Customer Contact, Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Annex 1 - Definitions

Term	Definition
Data Subjects	for the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information
Personal Data	means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Data Controllers	are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Law. We are the data controller of all personal data used in our business for our own commercial purposes
Processing	is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties
Workforce	Includes, any individual employed by [School/Trust] such as staff and those who volunteer in any capacity including Governors [and/or Trustees / Members/ parent helpers]

Annex 2 – SAR Acknowledgment Template (please share a copy with the DPO)

[On headed notepaper of data controller]

[DATE]

[ADDRESSEE]
[ADDRESS LINE 1]
[ADDRESS LINE 2]
[POSTCODE]

Dear [NAME],

Acknowledgment of your data subject access request

Name of Data Subject: [NAME]

I write to acknowledge receipt of your request for personal information, on the data subject named above, which we are responding to under article 15 of the General Data Protection Regulation.

- Your request was received on [DATE]
- ID was received on [DATE] (If applicable)
- Consent from the data subject was received on [DATE] (If applicable)

[Use if we can respond within one month]: Unless there are grounds for extending the statutory deadline of one calendar month, we expect to be able to provide you with a full response by [DATE].
or
[Use if complex and we need to extend the timescale]: As this SAR contains [sensitive Safeguarding information/has been received at the end of term/during school closure] it has been deemed to be complex and the timeline has been extended from one month by a further two months and we will provide you with a full response by [DATE].

As agreed, your preferred format for receiving this data is [paper copy/electronic copy].

We will now conduct a reasonable and proportionate search, we will focus the search on: [the School Information Management System/Safeguarding system/pupil file].

Yours sincerely,

[NAME OF SENDER]

For and on behalf of [Trust/School]

Annex 3 – SAR Response Template (please share a copy with the DPO)

[On headed notepaper of data controller]

Date

[ADDRESSEE]
[ADDRESS LINE 1]
[ADDRESS LINE 2]
[POSTCODE]

Dear [Name]

Response to your data subject access request

This letter is in response to your Subject Access Request received on **[Date]** in relation to [Name].

In line with the UK GDPR, a reasonable and proportionate search has been undertaken, and the following documents have been provided in paper/electronic format:

- School Information Management System
- Safeguarding System
- Pupil File

As part of the reasonable and proportionate search the date range for information included is:

Third party data has been redacted where we do not have consent to share the information with you. Data outside the scope of the request may have been redacted.

Information has not been disclosed where the following exemption exists:

- Insert as appropriate and discuss with DPO.
- E.g. Crime & Taxation exemption
- Child abuse data where disclosure is not in the best interests of the child

The purposes for which the personal data is processed:

- where we are required to by law
- To carry out a task in the public interest
- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to safeguard pupils
- to assess the quality of our services
- to comply with the law regarding data sharing

- to aid in the prevention and detection of crime on the Academy/School/Trust site
- where we have consent
- To provide or obtain additional services including advice and/or support for your family
- To enable payments to be made by you to the Academy/School/Trust

The recipients or classes of recipients of personal data to whom the data has been or will be disclosed and the location of any recipients outside the EEA:

- schools that the pupil's attend after leaving us
- our local authority
- the Department for Education (DfE)
- the school nursing service/medical/doctors/health care providers
- Nottingham Catholic Diocese

The categories of personal data concerned:

- Personal information (such as name, unique pupil number and address, parent contact details)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information (such as exam and test results)
- Relevant medical information
- CCTV footage & photographs
- Special Educational Needs information
- financial details such as eligibility for free school meals or other financial assistance
- Parent relationship to your child, including any Court orders that may be in place

Sources of personal data:

- Data subject/Parent/Carer
- Local Authority
- Other Schools
- Medical/Doctors/Health care providers
- Other professional bodies

You have the following rights under the GDPR:

- the right to request rectification of inaccurate personal data;
- In limited circumstances, the right to:
- request erasure of the personal information;
- request restriction of processing of the personal information; or

- object to the processing of the personal information

This subject access request is now complete. If you are unhappy with this response, and believe the school has not complied with legislation, please ask for a review by following our data protection complaints process; or by contacting myself at the school (INSERT NAME & Tel No. XXXX) or Trust DPOs, Tamer Robson & Teresa Bettelley (Tel: 0115 8515454).

If you still remain dissatisfied following an internal review, you can appeal to the Information Commissioner, who oversees compliance with data protection law. You should write to: Customer Contact, Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Yours sincerely

[NAME]
[For and on behalf of [Trust/Academy/School]

Annex 4 – Fees Table for Administrative Costs of Excessive SARs

What is included in the Administration Fee for excessive SARs?

This includes:

- Staff time:
  - assessing whether or not the school/Trust is processing the information
  - locating, retrieving and extracting the information
  - IT time for the data trawl
  - Staff time to collate the information they hold (if applicable)
  - GDPR Lead time to collate the data, read, redact, photocopy, scan, proofread etc.
  - DPO time to support in the redaction and proof-reading process
  - Legal advisors time (if applicable)
  - communicating the response to the individual, including contacting the individual to inform them that you hold the requested information
- Material costs:
  - IT and system use
  - Photocopying costs per A4 page
  - Printing costs per A4 page
  - Postage costs (if applicable) including envelopes etc.
  - Redaction material costs

Time calculated based on:

- Gathering relevant data
- Reading data and removing anything not relevant to the request – 10 pages per hour
- Redacting - 10 pages per hour
- DPO checking redactions - 10 pages per hour

Fees Table

Category	Cost
Staff time (school)	£15 per hour
Staff time (DPO)	£20 per hour
Photocopying	1p per A4 page
Printing	5p per A4 page
IT and system use	£1 per hour
Postage	Exact costs

For excessive SARs a fee will only be charged for the administrative costs in excess of 14 hours; the first 14 hours will not be charged for.