



# NPAT SUBJECT ACCESS REQUEST POLICY

Associated Policies:	
Author:	
Date Approved:	Nov 2021
Approved by:	Board of Trustees
Date issued:	23 <sup>rd</sup> Nov 2021
Date of Review:	Nov 2024
Website Inclusion	Y
Version:	V1.0 23

## CONTENTS

Contents .....	1
1. Policy statement .....	2
Who does this policy apply to .....	2
Policy review arrangements .....	2
2. Definition of data protection terms .....	2
3. Recognising a subject access request.....	2
4. Verifying the identity of a requester.....	3
5. Fee for responding to requests.....	3
6. Time period for responding to a SAR .....	4
7. Form of response .....	4
8. Sharing information with third parties.....	4
9. Withholding information .....	5
10. Process for dealing with a Subject Access Request.....	6

## 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 Northampton Primary Academy Trust (NPAT).

## WHO DOES THIS POLICY APPLY TO

All data subjects of Northampton Primary Academy Trust.

## POLICY REVIEW ARRANGEMENTS

This policy will be reviewed and updated as necessary if/when any changes are made to legislation that affect our Trust's practice. Otherwise, or from then on, this policy will be reviewed every 3 years and shared with the full Trust board.

## 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 NPAT processes personal data concerning data subjects, those data subjects have the right to access that personal data under UK 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 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 Data Protection Officer ("DPO") as soon as possible.

3.5. In order that the trust is properly able to understand the nature of any SAR and to verify the identity of the requester, any requester making a request verbally should be logged by a member of staff writing and direct this to the DPO.

3.6. A SAR will be considered and responded to in accordance with the UK 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 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 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 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

## 5. FEE FOR RESPONDING TO REQUESTS

5.1. The trust will usually deal with a SAR free of charge.

5.2. Where a request is considered to be manifestly unfounded or excessive a fee may be requested. Alternatively, the trust may refuse to respond to the request. If a request is considered to be manifestly unfounded or unreasonable the trust will inform the requester why this is considered to be the case.

5.3. 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.

## 6. TIME PERIOD FOR RESPONDING TO A SAR

6.1. The trust 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, or c. payment of any required fee.

6.2. In circumstances where the trust 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 of the data subject has been received (see below in relation to sharing information with third parties).

6.3. 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. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.

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

6.5. A request may be received during or less than one month prior to a school holiday. Where a request is made prior to a holiday period the trust will seek to respond prior to that holiday commencing, however where this is not possible then the trust will inform the requester that this is the case.

## 7. FORM OF RESPONSE

7.1. A requester can request a response in a particular form. 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.

## 8. SHARING INFORMATION WITH THIRD PARTIES

8.1. 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).

8.2. 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 should not approach the data subject directly but should inform the requester that it cannot respond without the written authorisation of the data subject.

8.3. If the trust 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.

8.4. 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.

8.5. 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 is confident that the child can understand their rights. Generally, where a child is under 12 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.

8.6. In all cases the trust should consider the particular circumstances of the case, and the above are guidelines only.

## 9. WITHOLDING INFORMATION

9.1. 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.

9.2. Where the information sought contains the personal data of third-party data subjects then the trust will:

9.2.1. 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;

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

9.2.3. 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.

9.3. So far as possible the trust will inform the requester of the reasons why any information has been withheld.

9.4. Where providing a copy of the information requested would involve disproportionate effort the trust will inform the requester, advising whether it would be possible for them to view the documents at the trust 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.

9.5. 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. PROCESS FOR DEALING WITH A SUBJECT ACCESS REQUEST

10.1. When a subject access request is received, the trust will:

10.1.1. notify the DPO who will be responsible for managing the response;

10.1.2. [subject to para 6.6 above,] acknowledge receipt of the request and provide an indication of the likely timescale for a response within 5 working days (see template at Annex 3);

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

10.1.4. 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;

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

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

10.1.7. Ensure the DPO has reviewed the information before disclosure can take place

10.1.8. 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 4); and

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

## Appendix 1 Definitions

<b>Term</b>	<b>Definition</b>
Data Subjects	for the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, parents, our workforce, staff, volunteers, 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 UK 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 NPAT such as staff and those who volunteer in any capacity including Governors and/or Trustees / Members/ parent helpers



## Appendix 2 SAR acknowledgement

**(for use over holidays when the School is closed for over a month)**



Dear [DATA SUBJECT],

[DATE]

Acknowledgement of your data subject access request dated [DATE OF REQUEST] and notification that the [School/Academy] is currently closed.

We write further to your request for details of personal data which we received on [DATE OF REQUEST]. As advised in [INSERT HERE HOW AND WHEN THE DATA SUBJECT WAS ADVISED OF THE DATES THE SCHOOL WOULD BE CLOSED] the [School/Academy] is [closing / closed] from xx July 21xx until xx September 21xx. Accordingly, the information you have requested is not accessible, and we will unfortunately not be able to comply with your request within one month. [OR We are unfortunately only able to provide you with the enclosed information as the remainder of the information is not accessible] The [School / Academy] will be reopening on xx September 20xx when your request will be formally acknowledged, and you will be informed about the timeframe in which a full response to your request will be provided. We apologise for any inconvenience this may cause and will contact you again on xx September 20xx.

Yours sincerely,

[NAME OF SENDER]

For and on behalf of Trust

## Appendix 3 SAR response template



Dear [DATA SUBJECT],

[DATE]

Response to your data subject access request dated [DATE OF REQUEST]

We write further to your request for details of personal data which we hold [and our acknowledgment of [DATE WHEN REQUEST FIRST ACKNOWLEDGED BY LETTER]].

We enclose all of the data to which you are entitled under the UK General Data Protection Regulation (GDPR), in the following format:

Your name	[Insert requester's name]
Your relationship with the school	[Pupil / parent / employee / governor / volunteer / other (specify)]
Details of the information you requested/enclosed	[Insert details of the specific information requested, such as: Your personnel file Your child's medical records Your child's behaviour record, held by [insert class teacher] Emails between 'A' and 'B' between [date]]
Date we supplied the information	[This must be within one month of the above date, except in the case of an extension or delay, e.g. in receiving ID]
Format we supplied the information	

You will note that some of the information has been redacted. The reason for this is that the redacted information relates to [a] third part[y/ies] who have not consented to the sharing of their information with you].

[Some information has not been provided as it is covered by the following exemptions:

**LIST EXEMPTIONS APPLIED]**

If you are unhappy with this response, and believe trust has not complied with legislation, please ask for a review by [following our complaints process; details can be found on our website at [LINK] OR by contacting [INDIVIDUAL (COULD BE DPO OR OTHER APPROPRIATE POSITION)]].

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 NPAT