GDPR SUBJECT ACCESS REQUEST TOOLKIT

Northgate Primary School

INTRODUCTION / OVERVIEW

1. The GDPR extends to all data subjects a right of access to their own personal data. This is known as a Subject Access Request (SAR). A formal request from a data subject for information that a school holds about them must be made in writing or electronically. A school / academy can invite a data subject to complete a form but cannot insist that they do so. A subject access request can be made by anyone including pupils, parents, staff, governors and members of the public.

2. It is important that all members of staff are able to recognise that any written request made by a person for their own information is likely to be a valid subject access request, even if the individual does not specifically use this phrase in their request or refer to the GDPR. In some cases, an individual may mistakenly refer to the "Freedom of Information Act" but this should not prevent the school from identifying the request as being made under the GDPR if appropriate. Some requests may be a combination of a subject access request for personal data under the GDPR and a request for information under the Freedom of Information Act 2000 ("FOIA"). Requests for information under the FOIA must be dealt with promptly and in any event within 20 school days.

3. Any member of staff who receives a written request for personal data must immediately forward it to the school's DPO as the statutory time limit for responding under the GDPR is **one calendar month** from receipt. Previously under the Data Protection Act 1998, Data Controllers had 40 calendar days to respond to a request. The timescales for responding **do not pause** when the school is closed for holidays, unlike the FOIA.

4. A fee may no longer be charged to the individual for provision of this information (previously a fee of £10 could be charged under the Data Protection Act 1998). The school must provide a copy of the information free of charge. However, it is possible to charge a 'reasonable fee' when a request is "manifestly unfounded or excessive", particularly if it is repetitive. It is advisable for the school to consult any guidance issued by the Information Commissioner's Office (ICO) on what is deemed to be "manifestly unfounded or excessive" before relying on this exemption, particularly as it is likely to be a high threshold to satisfy.

The school may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that the school can charge for all subsequent access requests.

The fee must be based on the administrative cost of providing the information.

5. The school may ask the Data Subject for reasonable identification so that they can satisfy themselves about the person's identity before disclosing the information.

6. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place. Certain information may be exempt from disclosure so it will be necessary to consider the exemptions that might apply. In practice, this means that the school may be entitled to withhold some documents entirely or may need to redact parts of them. Care should be taken to ensure that documents are redacted properly. Please seek further advice or support from the school's DPO if unsure which exemptions apply.
7. Requests from pupils who are considered mature enough to understand their rights to access their data should be processed as a subject access request and the data should be given directly to the pupil (subject to any exemptions that apply under the Act or other legislation). It may be reasonable to adopt a presumption that by the age of 13 a child has sufficient maturity to understand their rights and to make an access request themselves if they wish. In every case it will be for the school, as data controller, to assess whether the child is capable of understanding their rights under the Act and the implications of their actions, and so decide whether the parent needs to make the request on the child's behalf. A parent would normally be expected to make a request on a child's behalf if the child is younger than 13 years of age (subject to any court orders which may be in place).

8. Subject access requests from parents in respect of their own child where a child does not have sufficient maturity to understand their rights should be processed as requests made on behalf of the data subject (the child), subject to any court orders which may be in place. Where the school considers the child to be mature enough to understand their rights to request their data following receipt of a request from a parent, the school trust should ask the child for their consent to disclosure of the personal data (subject to any enactment or guidance which permits the school to disclose the personal data to a parent without the child's consent). Subject to the paragraph below, if consent is not given to disclosure, the school should not disclose the personal data if to do so would breach any of the data protection principles. Subject to some exceptions, schools can usually continue to share information about pupils with parents in the context of the day to day running of the school without needing to obtain pupils' consent. The reference to obtaining consent in this paragraph applies if a parent has made a subject access request for their child's personal data and the child is mature enough to exercise their own rights. If the school is unsure what to do in these circumstances, they should obtain legal advice.

9. It should be noted that the Education (Pupil Information) (England) Regulations 2005 give parents of children who attend maintained schools a right to access their child's educational records. This means that if a parent of a child at a maintained school submits a written request for a copy of their child's educational record, the school must respond within 15 school days. This is a separate statutory right that parents have aside from the DPA 2018, subject to any court orders which may be in place.

10. As the Education (Pupil Information) (England) Regulations 2005 do not apply to academies, requests for educational records from parents of children who attend academies must be dealt with under the DPA 2018 (as outlined above). This is without prejudice to the obligation on the academy trust in the Education (Independent School Standards) (England) Regulations 2014 to provide an annual report of each registered pupil's progress and attainment in the main subject areas taught to every parent (unless they agree otherwise in writing).

11. Following receipt of a subject access request, and provided that there is sufficient information to process the request, an entry should be made in the school's subject access log book, showing the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (e.g. Student Record, Personnel Record), and the planned date for supplying the information (not more than one calendar month from the request date). Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be the date on which sufficient information has been provided.

12. In the context of a school a subject access request is often wrapped up in a broader complaint or concern from a parent or may be connected to a disciplinary or grievance for an employee. The school should therefore ensure that the broader context is taken into account when responding to a request and seek advice if required on managing the broader issue and the response to the request.

This overview is not intended to be an exhaustive statement of the law and should not be relied on as legal advice to be applied to any particular set of circumstances. Instead, it is intended to act as a brief introductory view of some of the legal considerations relevant to the subject in question.

CHECKLIST FOR SCHOOLS

Following receipt of a Subject Access Request (SAR), schools/academies should use the following checklist as a guide:

A. Subject Access Requests Checklist	
Inform data subjects of their right to access data in your privacy notice and provide an easily accessible mechanism through which such a request can be submitted (e.g. a dedicated email address). You cannot insist that people use this method or refuse to respond if they send a request using a different method. Consider any steps you can take to mitigate any risk to the school if the timescales for responding to a subject access request includes the school holidays.	
Make sure an SAR policy is in place within the school and that internal procedures on handling of SARs are accurate and complied with. Include, among other elements, provisions on; a. Responsibilities (who, what) b. Timing c. Changes to data d. Handling requests for rectification, erasure or restriction of processing.	
Ensure personal data is easily accessible at all times in order to ensure a timely response to SARs and that personal data on specific data subjects can be easily filtered. Ensure staff are trained to extract reports from the MIS system, as well as any other 3rd party software, following receipt of an SAR.	
B. Steps to take following receipt of an SAR	
Verify whether you are controller of the data subject's personal data. If you are not a controller, but merely a processor, inform the data subject and refer them to the actual controller.	
Verify the identity of the data subject; if needed, request any further evidence on the identity of the data subject. If the request is from a parent for their child's data, consider whether the pupil has sufficient maturity to exercise their own rights (usually from the age of 13). If so, establish whether the pupil gives their consent to their personal data being disclosed to the parent. Establish whether there are any court orders in place. [For maintained schools only - Also consider whether the request falls within the remit of the Education (Pupil Information) (England) Regulations 2005.]	

Verify the access request; is it sufficiently substantiated? Is it clear to the data controller what information is requested? If not, request additional information.	
Ensure data will not be changed as a result of the SAR. Routine changes as part of the processing activities concerned are permitted.	
Verify whether the data requested also involves data on other data subjects and check if this data needs to be redacted before the requested data is supplied to the data subject if the other data subjects have not consented to the supply of their data as part of the SAR. Consider whether any other exemptions apply to the data and have particular regard to whether any safeguarding concerns could arise if the information is disclosed. Seek further advice from the DPO if you are in any doubt.	
C. Responding to an SAR	
Make sure to respond to an SAR within one calendar month after receipt of the request: a. If more time is needed to respond to complex requests, an extension of another two months is permissible, provided this is communicated to the data subject in a timely manner within the first month; b. If you do not take action on the request of the data subject, inform the data subject on this decision without delay and at the latest within one month of receipt of the request.	
If an SAR is submitted in electronic form, any information should preferably be provided by electronic means as well.	
If data on the data subject is processed, make sure to include as a minimum the following information in the SAR response: a. the purposes of the processing; b. the categories of personal data concerned; c. the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules or EC model clauses; d. where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period; e. the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;	

f. the right to lodge a complaint with a supervisory authority (i.e. the ICO); g. if the data has not been collected from the data subject: the source of such data; h. the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.	
Provide a copy of the personal data undergoing processing (subject to any exemptions which entitle you to withhold personal data). This should be provided in a commonly used electronic form if the data subject has submitted the SAR electronically.	

Guidance for Staff on Responding to a Subject Access Request

What Must I Do?

1. On receipt of a subject access request you must **forward** it immediately to Julie Lane, Deputy DPO, Business Manager at julie.lane@northgate.herts.sch.uk who will then inform the DPO.
2. We must correctly **identify** whether a request has been made / ensure that it is not being confused with the rights that people have to request information under the Freedom of Information Act 2000.
3. Any employee who receives a request to locate and supply information relating to an SAR must make a full exhaustive **search** of the records to which they have access.
4. All the information that has been requested must be **provided** unless an exemption can be applied.
5. We must **respond** within one calendar month after accepting the request as valid.
6. Subject Access Requests must be undertaken **free of charge** to the requester
7. Line managers must ensure that the staff they manage are **aware** of and follow this guidance.
8. Where a requester is not satisfied with a response to an SAR, the School must manage this in accordance with its complaints policy.

How Must I Do it?

1. We must ensure a request has been received in writing where a data subject is asking for sufficiently well-defined personal data held by the School relating to themselves.
2. The Act permits and encourages us to clarify with the requester what information they need. They must supply their address and valid evidence to prove their identity. The School accepts the following forms of identification (* these documents must be dated in the past 12 months, + these documents must be dated in the past 3 months):

    - Current UK/EEA Passport
    - UK Photocard Driving Licence (Full or Provisional)
    - Firearms Licence / Shotgun Certificate
    - EEA National Identity Card
    - Full UK Paper Driving Licence
    - State Benefits Entitlement Document*
    - State Pension Entitlement Document*
    - HMRC Tax Credit Document*
    - Local Authority Benefit Document*
    - State/Local Authority Educational Grant Document*
    - HMRC Tax Notification Document
    - Disabled Driver's Pass
    - Financial Statement issued by bank, building society or credit card company+
    - Judiciary Document such as a Notice of Hearing, Summons or Court Order
    - Utility bill for supply of gas, electric, water or telephone landline+
    - Most recent Mortgage Statement

- Most recent Council Tax Bill / Demand or Statement
- Current Council Rent Card
- Current Council Tenancy Agreement
- Building Society Passbook which shows a transaction in the last 3 months and your address

3. Depending on the degree to which information is organised and structured, you will need to search the following non-exhaustive areas: MIS system, 3rd party software (including apps), emails (including archived emails and those that have been deleted but are still recoverable), Word documents, spreadsheets, databases, systems, CCTV, removable media (for example, memory sticks, floppy disks, CDs), tape recordings, paper records in relevant filing systems etc. which your area is responsible for or owns.

4. You must not withhold information because you believe it will be misunderstood; instead, you should provide an explanation with the information. You must provide the information in an 'intelligible form', which includes giving an explanation of any codes, acronyms and complex terms. The information must be supplied in a permanent form except where the person agrees or where it is impossible or would involve undue effort. You may be able to agree with the requester that they will view the information on screen or inspect files on our premises. You must redact any exempt information from the released documents and explain why that information is being withheld.

5. By ensuring that DPO has logged the request, we can ensure that we respond within the statutory timescales.

6. As the time for responding to a request does not stop during the periods when the school is closed for the holidays, we will attempt to mitigate any impact this may have on the rights of data subjects to request access to their data by implementing the following measures:

    - A designated email address is setup for data subject requests: gdpr@northgate.herts.sch.uk

    - The email address is checked once a week during school holiday periods by the Deputy DPO.

    - Any requests are immediately passed to / discussed with the DPO and any relevant action taken.

    - When an email is received a message is automatically sent to the Deputy DPO

7. When responding to a complaint, we must advise the requester that they may complain to the ICO if they remain unhappy with the outcome.

Sample Letters Responding to a Subject Access Request

The letters below are samples and do not cover every eventuality to reflect local circumstances nor have they been drafted or tailored for a school's specific needs, so they should not be relied on as legal advice to be applied to any particular set of circumstances. They should be tailored to reflect the context under which the subject access request has arisen and legal advice should be sought if required.

All Letters Must Include the Following Information:

a. the purposes of the processing;

b. categories of personal data concerned;

c. the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules or EC model clauses;

d. where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;

e. the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

f. the right to lodge a complaint with a supervisory authority;

g. if the data has not been collected from the data subject: the source of such data;

h. the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

A. Replying to a Subject Access Request Providing the Requested Information

[Name] [Address]

[Date]

Dear *[Name of data subject]*

Data Protection Act 2018 Subject Access Request

Thank you for your letter of *[date]* making a data subject access request for *[subject]*. We are pleased to enclose the information you requested.

[Include 1(a) to (h) above.]

[Copyright in the information you have been given belongs to the School or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published (including published on the Internet or an intranet), or otherwise made available in whole or in part without the prior written consent of the copyright holder.]

Yours sincerely

B. Release of Part of the Information, When the Remainder is Covered by an Exemption

[Name] [Address]

[Date]

Dear *[Name of data subject]*

Data Protection Act 2018 Subject Access Request

Thank you for your letter of *[date]* making a data subject access request for *[subject]*. To answer your request we asked the following departments to search their records for information relating to you:

- *[List the areas]*

I am pleased to enclose *[some/most of]* the information you requested. *[If any information has been removed]* We have removed any obvious duplicate information that we noticed as we processed your request, as well as any information that is not about you. You will notice that *[if there are gaps in the document]* parts of the document(s) have been redacted. *[OR if there are fewer documents enclose]* I have not enclosed all of the information you requested. This is because *[explain why it is exempt]*.

[Include 1(a) to (h) above.]

[Copyright in the information you have been given belongs to the School or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published (including published on the Internet or an intranet), or otherwise made available in whole or in part without the prior written consent of the copyright holder.]

Yours sincerely

C. Replying to a Subject Access Request Explaining Why You Cannot Provide Any of the Requested Information

[Name] [Address]

[Date]

Dear *[Name of data subject]*

Data Protection Act 2018 Subject Access Request

Thank you for your letter of *[date]* making a data subject access request for *[subject*].

I regret that we cannot provide the information you requested. This is because *[explanation where appropriate]*.

[Include 1(a) to (h) above if appropriate.]

Yours sincerely

D. Replying to a Subject Access Request Explaining Why You Have Only Sent Some of the Requested References

[Name] [Address]

[Date]

Dear [Name of data subject]

Data Protection Act 2018 Subject Access Request

Thank you for your letter of [date] making a data subject access request for the references we received in connection with your [job/course] application.

I enclose [whichever reference can be disclosed]. However, I have not provided [a copy/copies] of [one/some] of the references you requested because [one of your referees/your referees] withheld consent to disclose [it/them].

[Include 1(a) to (h) above.]

[Copyright in the information you have been given belongs to the School or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published (including published on the Internet or an intranet), or otherwise made available in whole or in part without the prior written consent of the copyright holder.]

Yours sincerely