<School Name>

SUBJECT ACCESS REQUEST PROCEDURE

INTRODUCTION / OVERVIEW

1. The GDPR (General Data Protection Regulation) extends to all data subjects a right of access to their own personal data. This is known as a subject access request. A formal request from a data subject (or parent/guardian/carer thereof) for information that a school holds about must be made in writing. A school can invite a data subject to complete a form but you 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 and the police/government agencies.

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 their personal data must inform the HT or Business Manager who will immediately forward it to the Trust DPO Alvin Walters (dpo@drbignitemat.org), as the statutory time limit for responding under the GDPR is **one calendar month** from receipt of the request. The timescales for SAR responses 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). You must provide a copy of the information free of charge. However, you can 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.

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

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

5. <School name> 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 you will need to consider what exemptions apply and decide whether you can rely on them. In practice, this means that you may be entitled to withhold some documents entirely or you may need to redact parts of them. Care should be taken to ensure that documents are redacted properly. Please seek further advice or support if you are 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.

9. As the Education (Pupil Information) (England) Regulations 2005 does 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).

10. 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 register which is located in the schools GDPRiS compliance system, 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.

11. In the context of a school, a subject access request is normally 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.

SCHOOL CHECKLIST

Following receipt of a Subject Access Request ('SAR'), school will:

A. Subject Access Requests Checklist	Tick (✓)
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/academy if the timescales for responding to a subject access request includes the school holidays.	
Make sure a 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 SIMs following receipt of a SAR.	
B. Steps to take following receipt of a SAR	**Tick (✓)**
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.	
SAR Response Team: Bring together the staff members appointed a part of the SAR Response Team. (HT, SBM, Safeguarding Lead, DPO, etc).	
Identification Verification: Verify the identity of the data subject; if needed, request any further evidence on the identity of the data subject.	
Requests comes from the Police (i): Police forces nationally are aware of the need to provide sufficient information to enable Data Controllers to make informed decisions. **Verify ID of the Requestor - Different forces take a slightly different approach, but broadly speaking the following information is always required:** • Who is the person making the request? • What is their rank or role within the organisation they represent? • The request must be signed and dated, electronically or hard copy **It should contain details of the information sought which should include:** • Name, date of birth and address of the data subject(s) (if known) – request should relate to the narrowest pool of people, ideally one person, to prevent risk of personal data disclosure on an unauthorised or an unlawful basis. • Summary of the information sought - Requests should be as specific as possible • An explanation why the requester believes the school has access to such information • Details of the issue that the information will address (if it is highly confidential or particularly sensitive the requester needs to explain why they cannot provide details) • Any timeframes or particular urgency.	

• Notification if they intend to share this with the data subject	
Requests comes from the Police (ii): The Data Controller may need to consider on what basis was information provided to them as controller in the first place. Questions to ask: • What might be the impact of releasing this information? • Is there a risk of causing harm to the third parties? • Would disclosing this information potentially lead to identification of a third party who is separate to the present enquiry? **Note:** In many cases, the answer is simple and straightforward. Schools as public authorities have a moral (and in some cases) legal obligation to assist and support law enforcement agencies. However, if there is any uncertainty about the nature, origin or reasons for a request then advice should be sought from the DPO. To emphasise, if this is a matter of life and limb always err on the side of caution. As police forces and other law enforcement agencies begin to acclimatise to the GDPR requirements it is likely we will see changes to processes, forms and procedures.	
If the request is from a parent/guardian 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.	
Verify the access request; is it sufficiently substantiated? Is it clear to the data controller what information is requested? If not, request additional information.	
Data gathering: You may need to search through Office 365 (SharePoint, email, OneDrive) or Cloud-based services used by the school (CPOMS, My Concern, etc) as well as paper records). Ensure data will not be changed as a result of the SAR. Routine changes as part of the processing activities concerned are permitted.	
Redaction: 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.	
Exemptions: 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 if you are in any doubt.	
C. Responding to a SAR	**Tick (✓)**
Make sure to respond to a 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; 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, using **Appendix C. Replying to a subject access request explaining why you cannot provide any of the requested information**	
If a 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 Standard Contractual Clauses (SSCs) or Binding Corporate Rules (BCRs); 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 (SAR)

What must I do?

1. On receipt of a subject access request, you must **forward** it immediately to the DPO Alvin Walters (dpo@drbignitemat.org)
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 a 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 of receipt of the request.
6. Subject Access Requests must be undertaken **free of charge** to the requestor
7. Line managers must ensure that the staff they manage are **aware** of and follow this guidance.
8. Where a requestor is not satisfied with a response to a 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 requestor what information they need. They must supply their address and valid evidence to prove their identity. If you have checked their identity before, visual person-to-person identification is acceptable, but you must make a note of this fact.

3. Depending on the degree to which information is organised and structured, you may need to search the following non-exhaustive areas:
    - *Office 365: [SharePoint, OneDrive, Emails (including archived emails and those that have been deleted but are still recoverable), Word/Excel/PowerPoint documents, spreadsheets, databases]
    - Cloud-based services/systems (CPOMS, My Concern, etc),
    - CCTV storage drive,
    - 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.

    Office 365 Security Centre (admin access only) has a Subject Access Request tool that can help with the search for all data in the Office 365 eco-system relating to a data subject. IT Manager and DPO will help with creating a case and running the DSR search.

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 the request has been reported to the DPO and the request recorded in GDPRiS, 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: The DPO will check their DPO e-mail addresses regularly during any holiday period.

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

Guidance: Responding to a Request from the Police

It is not uncommon for the police, or other prosecuting authorities, to request that schools share information with them as part of investigations to prosecute or in some cases actually prevent commission of crimes. When a school is asked for information it holds on their records it is being asked to disclose personal data and this data may be sensitive in nature. It may relate to a parent, carer or other family member of the pupil at school. It may relate to the pupil themselves.

Ensuring that the request is given appropriate consideration, and a suitable response is the obligation of the school acting as Data Controller.

Schedule 2, Part 1, paragraph 2 of the Data Protection Act 2018 replaces the old section 29(3) of the Data Protection Act 1998. In essence this provides an exemption for a Data Controller to provide personal, and even sensitive, data without breaching the principles of GDPR or falling foul of the sanctions in the Data Protection Act 2018. The principle behind this, is that good data protection regulations should not prevent detection of crime or be used to stop the apprehension or prosecution of offenders. There is also protection for organisations if there is a risk to the "vital interests" of a data subject or another party. This means that information can be shared if failing to do so would lead to risk of a serious injury or even death of an individual.

However, before deciding whether or not to disclose data, certain key elements of information are needed. Police forces nationally are aware of the need to provide sufficient information to enable Data Controllers to make informed decisions. Different forces take a slightly different approach, but broadly speaking the following information is always required:

- Who is the person making the request?
- What is their rank or role within the organisation they represent?
- The request must be signed and dated, electronically or hard copy

It should contain details of the information sought which should include:

- Name, date of birth and address of the data subject(s) *(if known)*
- Summary of the information sought
- An explanation why the requester believes the school has access to such information
- Details of the issue that the information will address *(if it is highly confidential or particularly sensitive the requester needs to explain why they cannot provide details)*
- Any timeframes or particular urgency.
- Notification if they intend to share this with the data subject

As a responder it is then necessary for the Data Controller to balance the request against the obligations set out in the GDPR and Data Protection Act 2018. PLEASE NOTE: Requests should be as specific as possible, and should relate to the narrowest pool of people, ideally one person, to prevent risk of personal data disclosure on an unauthorised or an unlawful basis. The Data Controller may need to consider on what basis was information provided to them as controller in the first place. Questions to ask:

- What might be the impact of releasing this information?
- Is there a risk of causing harm to the third parties?
- Would disclosing this information potentially lead to identification of a third party who is separate to the present enquiry?

In many cases, the answer is simple and straightforward. Schools as public authorities have a moral (and in some cases) legal obligation to assist and support law enforcement agencies. However, if there is any uncertainty about the nature, origin or reasons for a request then advice should be sought from the DPO. To emphasise, if this is a matter of life and limb always err on the side of caution. As police forces and other law enforcement agencies begin to acclimatise to the GDPR requirements it is likely we will see changes to processes, forms and procedures.

The Data Controller is legally responsible for taking care of personal and sensitive information about data subjects in their control. Providing information to the police is important but must be done with due consideration.

Appendix 9. Replying to a subject access request providing the requested information

*"[*N*ame]* [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"

Appendix B. Release of part of the information, when the remainder is covered by an exemption

*"[*N*ame]* [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"

Appendix C. Replying to a subject access request explaining why you cannot provide any of the requested information

*"[*N*ame]* [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

*"[*N*ame]* [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"

E. Subject Access Request Confirmation/Acknowledgement Letter

"[Name] [Address]

[Date]

Dear [name of data subject]

Data Protection Act 2018 subject access request

Reference: [DATA SUBJECT ACCESS REQUEST NUMBER****]**

We write to acknowledge receipt of your data subject access request under Article 15 of the General Data Protection Regulation (GDPR).

So that we may process your request, we would be grateful if you could provide confirmation of your identity in the form of [IDENTIFICATION REQUIRED].

Please also provide as much detail as possible about the information that you require, for example, name of the department and names of individuals where the information is most likely to be located, a particular service, period of time and incident.

Please note that we cannot supply the information you have requested until we have verified your identity. The deadline of 1 month in which to respond to your request will start to run as soon as we receive it. This deadline may also be extended by a further 2 months if your request is complex. We shall let you know if that is the case.

Your rights:

You have the right to:

- request the rectification/correction of your personal data
- request the restriction of our processing of your personal data
- object to our processing of your personal data

You also have the right to lodge a complaint with the Information Commissioners Office https://ico.org.uk/. Further details regarding our privacy practices can be found in our privacy policy *[add link to your school privacy policy here].*

The reference for your request is [DATA SUBJECT ACCESS REQUEST NUMBER] and please quote this on all correspondence concerning this request.

1.1 Document Control

The Data Protection Officer is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the GDPR.

A current version of this document is available to all/specified members of staff on the School and Trust websites.

This procedure was approved by the Chief Executive Officer (CEO) or Trust Chair and is issued on a version-controlled basis under his signature.

Name	Signature	Date
David Sheldon		16/11/2020

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	Richard Martin	3/5/2018
2	Review & update	David Sheldon	16/11/2020