Appendix 1 – Subject Access Requests

Under Data Protection Law, data subjects have a general right to find out whether the Trust hold or process personal data about them, to access that data, and to be given supplementary information. This is known as the right of access or the right to make a data subject access request (SAR). The purpose of the right is to enable the individual to be aware of and verify the lawfulness of the processing of personal data that the Trust are undertaking.

This appendix provides guidance for staff members on how data subject access requests should be handled and for all individuals on how to make a SAR.

A data subject has the right to be informed by the Trust of the following: -

(a) Confirmation that their data is being processed;

(b) Access to their personal data;

(c) A description of the information that is being processed;

(d) The purpose for which the information is being processed;

(e) The recipients/class of recipients to whom that information is or may be disclosed;

(f) Details of the Trust's sources of information obtained;

(g) In relation to any personal data processed for the purposes of evaluating matters in relation to the data subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting them, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct; and

(h) Other supplementary information.

How to Recognise a Subject Access Request

A data subject access request is a request from an individual (or from someone acting with the authority of an individual, e.g., a solicitor or a parent making a request in relation to information relating to their child):

- for confirmation as to whether the Trust process personal data about them and, if so
- for access to that personal data
- and/or certain other supplementary information

A valid SAR can be both in writing (by letter, email, WhatsApp text) or verbally (e.g., during a telephone conversation). The request may refer to the UK GDPR and/or to 'data protection' and/or to 'personal data' but does not need to do so in order to be a valid request. For example, a letter which states 'please provide me with a copy of information that the Trust hold about me' would constitute a data subject access request and should be treated as such.

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

What to do When You Receive a Data Subject Access Request

All data subject access requests should be immediately directed to the school's Headteacher (or to the Director of Resources for Trust SARs) who should contact the DPO in order to assist with the request and what is required.

Acknowledging the Request

When receiving a SAR the Trust shall acknowledge the request as soon as possible and inform the requester about the statutory deadline (of one calendar month) to respond to the request.

In addition to acknowledging the request, the Trust may ask for:

- proof of ID (if needed);
- further clarification about the requested information;
- if it is not clear where the information shall be sent, the Trust must clarify what address/email address to use when sending the requested information; and/or
- consent (if requesting third party data).

The Trust should work with their DPO in order to create the acknowledgment.

Verifying the Identity of a Requester or Requesting Clarification of the Request

Before responding to a SAR, the Trust will take reasonable steps to verify the identity of the person making the request. In the case of current employees, this will usually be straightforward. 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. 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 a passport, driving license, a recent utility bill with current address, birth/marriage certificate, credit card or a mortgage statement.

If an individual is requesting a large amount of data the Trust may ask the requester for more information for the purpose of clarifying the request, but the requester shall never be asked why the request has been made. The Trust shall let the requestor know as soon as possible where more information is needed before responding to the request.

In both cases, the period of responding begins when the additional information has been received. If the Trust do not receive this information, they will be unable to comply with the request.

Requests Made by Third Parties or on Behalf of Children

The Trust need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney. The Trust may also require proof of identity in certain circumstances.

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.

When requests are made on behalf of children, it is important to note that even if a child is too young to understand the implications of subject access rights, it is still the right of the child, rather than of anyone else such as a parent or guardian, to have access to the child's personal data. Before responding to a SAR for information held about a child, the Trust should consider whether the child is mature enough to understand their rights. If the Trust is confident that the child can understand their rights, then the Trust should usually respond directly to the child or seek their consent before releasing their information.

It shall be assessed if the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, it should be taken into account, among other things:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

Generally, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. In relation to a child 12 years of age or older, then provided that the Trust 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 will require the written authorisation of the child before responding to the requester or provide the personal data directly to the child.

The Trust may also refuse to provide information to parents if there are consequences of allowing access to the child's information – for example, if it is likely to cause detriment to the child.

Fee For Responding to a SAR

The Trust will usually deal with a SAR free of charge. Where a request is considered to be manifestly unfounded or excessive a fee to cover administrative costs may be requested. 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 and that the Trust will charge a fee for complying with the request.

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.

If a fee is requested, the period of responding begins when the fee has been received.

Time Period for Responding to a SAR

The Trust has one calendar month to respond to a SAR. This will run from the day that the request was received or from the day when any additional identification or other information requested is received, or payment of any required fee has been received.

The 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.

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.

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

Trust Closure Periods

The Trust may not be able to respond to requests received during or just before school closure periods within the one calendar month response period. This is because schools will be closed. As a result, it is unlikely that your request will be able to be dealt with during this time. We may not be able to acknowledge your request during this time (i.e., until a time when we receive the request). However, if we can acknowledge the request, we may still not be able to deal with it until the schools re-open. The Trust will endeavour to comply with requests as soon as possible and will keep in communication with you as far as possible. If your request is urgent, please provide your request during term times and not during/close to closure periods.

Information to be Provided in Response to a Request

The individual is entitled to receive access to the personal data we process about them and the following information:

- the purpose for which we process the data;
- the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular where those recipients are in third countries or international organisations;
- where possible, the period for which it is envisaged the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the fact that the individual has the right:
    - to request that the Company rectifies, erases or restricts the processing of his personal data; or
    - to object to its processing;
    - to lodge a complaint with the ICO;
    - where the personal data has not been collected from the individual, any information available regarding the source of the data;
    - any automated decision we have taken about them together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for them.

The information should be provided in a way that is concise, transparent, easy to understand and easy to access using clear and plain language, with any technical terms, abbreviations or codes explained. The response shall be given in writing if the SAR was made in writing in a commonly used electronic format.

The information that the Trust are required to supply in response to a SAR must be supplied by reference to the data in question at the time the request was received. However, as the Trust have one month in which to respond the Trust is allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data is supplied if such amendment or deletion would have been made regardless of the receipt of the SAR.

Therefore, the Trust is allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of a SAR. The Trust is not allowed to amend or delete data to avoid supplying the data.

How to Locate Information

The personal data the Trust need to provide in response to a data subject access request may be located in several of the electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

Depending on the type of information requested, the Trust may need to search all or some of the following:

- electronic systems, e.g., databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data, CCTV;
- manual filing systems in which personal data is accessible according to specific criteria, e.g., chronologically ordered sets of manual records containing personal data;
- data systems held externally by our data processors;
- occupational health records;

- pensions data;
- share scheme information;
- insurance benefit information.

The Trust should search these systems using the individual's name, employee number or other personal identifier as a search determinant.

Protection of Third Parties - Exemptions to the Right of Subject Access

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

The Trust will consider whether it is possible to redact information so that this does not identify those third parties. If their data cannot be redacted (for example, after redaction it is still obvious who the data relates to) then the Trust do not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information unless:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information without the individual's consent, all of the relevant circumstances will be taken into account, including:

- the type of information that they would disclose;
- any duty of confidentiality they owe to the other individual;
- any steps taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

It needs to be decided whether it is appropriate to disclose the information in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to the Trust disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, the Trust must decide whether to disclose the information anyway. If there are any concerns in this regard then the DPO should be consulted.

Other Exemptions to the Right of Subject Access

In certain circumstances the Trust may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

Crime detection and prevention: The Trust do not have to disclose any personal data being processed for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty.

Confidential references: The Trust do not have to disclose any confidential references given to third parties for the purpose of actual or prospective:

- education, training or employment of the individual;
- appointment of the individual to any office; or
- provision by the individual of any service

This exemption does not apply to confidential references that the Trust receive from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (i.e., the person giving the reference), which means that the Trust must consider the rules regarding disclosure of third-party data set out above before disclosing the reference.

Legal professional privilege: The Trust do not have to disclose any personal data which is subject to legal professional privilege.

Management forecasting: The Trust do not have to disclose any personal data processed for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity.

Negotiations: The Trust do not have to disclose any personal data consisting of records of intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

Refusing to Respond to a Request

The Trust can refuse to comply with a request if the request is manifestly unfounded or excessive*,* taking into account whether the request is repetitive in nature.

If a request is found to be manifestly unfounded or excessive the Trust can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

In either case the Trust need to justify the decision and inform the requestor about the decision.

The reasonable fee should be based on the administrative costs of complying with the request. If deciding to charge a fee the Trust should contact the individual promptly and inform them. The Trust do not need to comply with the request until the fee has been received.

Record Keeping

A record of all subject access requests shall be kept with the DPO. The record shall include the date the SAR was received, the name of the requester, what data the Trust sent to the requester and the date of the response.