Inspiring Futures Through Learning

Subject Access Request Policy

April 2021 to April 2023

At Inspiring Futures through Learning, we are driven by our pursuit of excellence every day. We have high expectations of learning, behaviour and respect for every member of our community. We create independent, articulate thinkers and learners who have confidence in, not only their individual ambitions, but also those of the Academy and The Trust as a whole. We have collaboration at the heart of everything we do and our vision is to nurture exciting, innovative, outstanding Academies who embrace change and provide a world-class education for all it serves.

***Including all IFtL Schools, Milton Keynes Teaching School Alliance and Two Mile Ash Initial Teaching Training Partnership**

Policy name:		Subject Access Request Policy
Version:		V2
Date relevant from:		April 2021
Date to be reviewed:		April 2023 *This policy will be reviewed every two years unless legislation dictates otherwise. Recent changes in Legislation will need to be read and used to review this Policy.*
Role of reviewer:		IFtL Head of Operations
Statutory (Y/N):		Y
Published on website*:		3C

Policy level:**	1
Relevant to:	All employees through all IFtL schools and departments
Bodies consulted:	
Approved by:	IFtL Finance and Resources Committee
Approval date:	4th May 2021

Key:

**** Publication on website:***

IFtL website		**School website**	
1	Statutory publication	A	Statutory publication
2	Good practice	B	Good practice
3	Not required	C	Not required

***** Policy level:***

1. Trust wide:
   - This one policy is relevant to everyone and consistently applied across all schools and Trust departments with no variations.
     - *Approved by the IFtL Board of Trustees.*
2. Trust core values:
   - This policy defines the values to be incorporated fully in all other policies on this subject across all schools and Trust departments. This policy should therefore from the basis of a localised school / department policy that in addition contains relevant information, procedures and / or processes contextualised to that school / department.
     - *Approved by the IFtL Board of Trustees as a Trust Core Values policy.*
     - *Approved by school / department governance bodies as a relevantly contextualised school / department policy.*

3. School / department policies
   - These are defined independently by schools / departments as appropriate
     - *Approved by school / department governance bodies.*

Introduction

Under current data protection law, individuals have the right to access their personal data and the supplementary data that an organisation may hold about them.
As from May 25th 2018, subject access requests must, in most circumstances, be provided free of charge, within 1 month.
Exceptions can be made for requests that are 'excessive or manifestly unfounded'.
Where requests are made electronically, information should be provided in a commonly available machine readable format.

Responding to Subject Access Requests

Subject access requests should, ideally, be made using the form located in appendix 1 of this document. Requests made in other formats must also be actioned but, wherever possible, individuals should be asked to use the official form for consistency. Ideally, requests should be in writing but this cannot be enforced and verbal requests cannot be refused.
Where a verbal request is made, the person receiving the request and the school's appointed data lead should fill in the SAR template attached to this document to ensure that an appropriate record of the request is retained.
All subject access requests must be recorded on the school's GDPRiS system.

Requests may come in other formats, not always labelled as 'subject access requests'. For example, a parent may ask to see their child's behaviour record. This is effectively a subject access request and should be treated as such. Documentation that is provided as standard, as a part of the general school process, does not need to be treated as a SAR. For example, if a parent requests a copy of an EHCP and these are usually supplied to parents as standard practice, a request for a duplicate would not have to be treated as a subject access request and can simply be provided without having to go through the SAR procedure.

Unless a request has been made in person, contact should be made with the individual making the request to check that they have actually made this request themselves, to verify the identity of the individual, to acknowledge their request and inform them that it will be dealt with within 30 days.
You must identify the individual using 'reasonable means'. This term is not defined but, generally, this would involve seeing 2 forms of identification for the person and recording the

details.
In the case where a person is known to the school, for example, where a staff member or a known parent makes a subject access request, it is not necessary to obtain identification but you should obtain clarification from a second person to demonstrate that the applicant has been identified as known and record this on the form.
Requests must not be unduly delayed by excessive or unfounded requests for an individual to prove their identity. The legislation makes it clear that identity verification must be reasonable but any attempt to delay the request deliberately is a breach of the regulations.

All subject access requests must be approved by the trust's data protection officer. No information should be provided to individuals until the DPO has authorised its release.

Data Subjects and Data

Data subjects can request any personal data that an organisation holds about them. A data subject could be a pupil, a parent or carer, a staff member a visitor or a contractor.
Personal data relating to data subjects could be a name, photo, school report, register, medical information, safeguarding report, email relating to the data subject, recorded telephone conversation, CCTV image or any other data that refers to an identified, or identifiable, living individual.
There are some exclusions, particularly relating to safeguarding and child protection data, within the Data Protection Act 2018. Further guidance on this is available from the Data Protection Officer.

What Data Should be Provided?

Some requests can be very non-specific and if this proves to be too difficult to manage, you can ask the person making the request for further detail to make their request more specific. If the individual refuses to comply with this, you are still required to undertake reasonable efforts to find their information.
In addition to the data requested, you are also obliged to release the following information;
Why you are processing the data;
Who the data is shared with;
What your retention period is for the data concerned;
That the data subject has the right to rectification, erasure, restriction of, or objection to processing;

That the data subject has the right to complain to the ICO;
Information about the source of the data;
Whether the data is used in relation to automated decision making;
Any safeguards you use in transferring data to a third country or international organisation.

Much of this information is already in the IFtL privacy notices or policy document so it may be appropriate to include a copy of this within the requested information.
You also have a duty to explain any abbreviations or unusual terminology that may be included within the data.
Where a request is made for translation into another language, we are not required by law to provide this.

Unfounded or Excessive Requests

The terms 'unfounded' and 'excessive' are not defined under the legislation but can be interpreted as repetitive requests (where the individual repeatedly asks for copies of the same information) or requests where the scope of the data is far too broad to be collected. For example, where someone may ask for everything you have ever held about them across all of your systems.
Should an excessive or unfounded request be received you can either:

- Charge a reasonable fee for compliance based on the administrative costs of providing the information
- Refuse to comply, with an explanation for the refusal
- Comply within 3 months instead of the usual 1 month, but you must contact the individual to inform them of this and to explain why

You must not claim that a request is unfounded or excessive as a means of gaining more time to fulfil a request, or in order to allow a charge to be applied. Requests that are unnecessarily charged or extended may be reported to the ICO and can lead to prosecution of the data controller.

Requests Involving Information Relating to a Third Party

Where the data requested holds information regarding a third party, it is not always permitted to release this information without the consent of the third party.

In deciding whether or not we can honour this type of request, we need to consider the following;

- Does the request require the disclosure of the third party's information – can names or documents be removed from the scope of the request without compromising the overall request?
- Can we obtain consent from the third party to release their information?
- Would it be reasonable in all the circumstances, to disclose the information without the third party's consent anyway?

Cases will need to be assessed on an individual basis. For text-based documents, it may be possible to redact any information that we cannot share but for CCTV footage, for example, we are unlikely to have the appropriate technology to remove third parties from the footage, therefore we may not be permitted to release the data without consent, or we may decide that it is reasonable to release without consent.
Disclosure cannot simply be refused on the grounds that another person's data is included within the document as demonstrated in recent case law (http://www.bailii.org/ew/cases/EWCA/Civ/2018/1497.html)

Refusing a Request

When you refuse a request, you must;

- Respond within 1 month
- Explain why you are refusing the request
- Tell the individual that they have the right to complain to the ICO

Exemptions

There are some data that are exempt from the rules relating to subject access requests, most notably for schools, data concerning safeguarding and child protection.
The Data Protection Act 2018 sets out, within Schedule 3, specific criteria where certain data may be withheld following a subject access request.
For further guidance on this area, please consult with the trust's DPO.

Requests Made During Summer Holidays

The response time of 30 days is enforceable regardless of school holiday periods. This means that requests made during the summer break may be difficult to action within the allowed timeframe.
Where practical, a procedure should be put in place to ensure that emails are monitored through the summer holidays and are appropriately responded to.
A line should be added to privacy notices stating that while we are happy to assist people in accessing their information in a timely manner, we will find it difficult to respond during the summer holidays (as recommended by the DfE).

Evidencing SARs

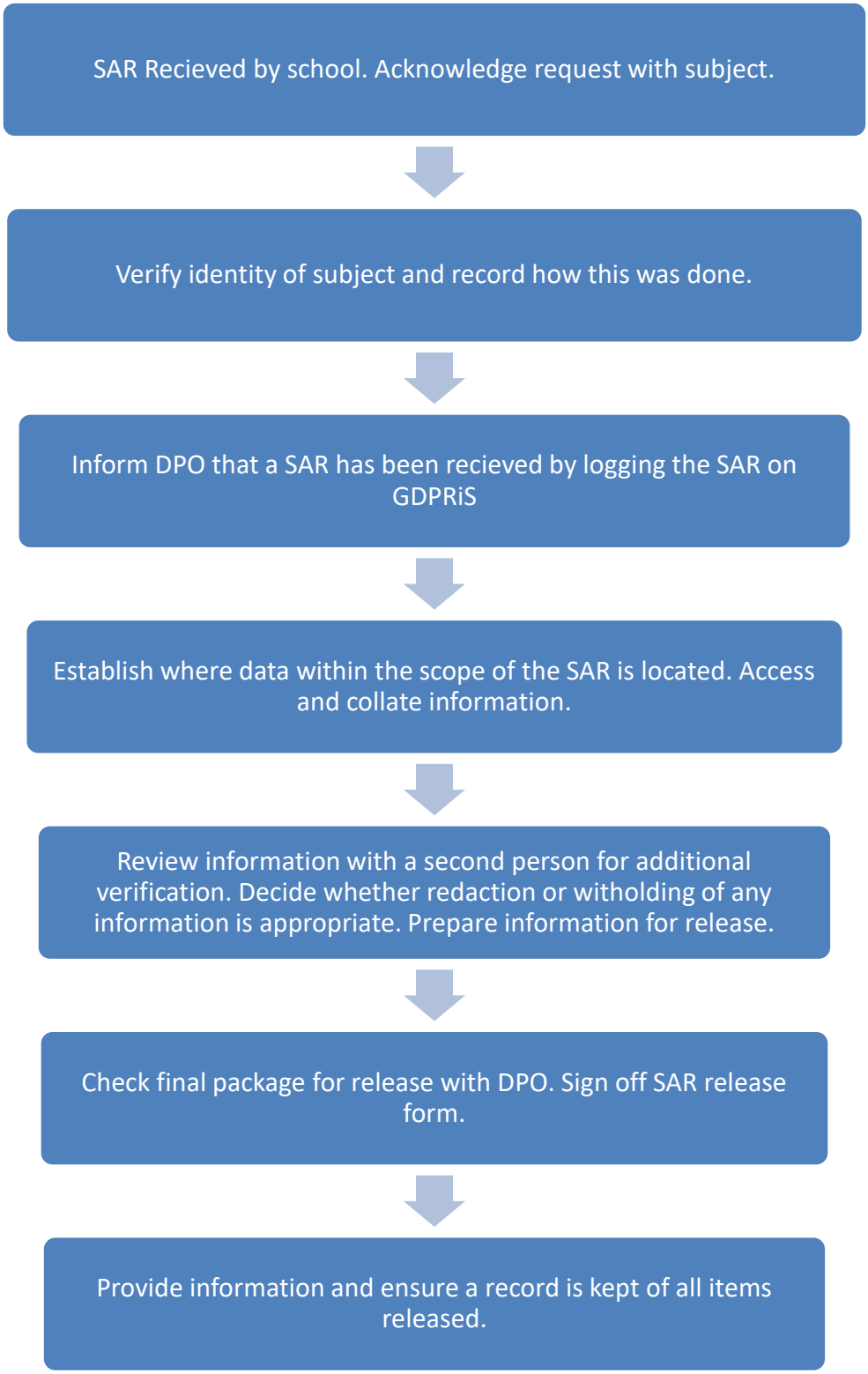
As well as a copy of the SAR form, you should also keep a copy of the data provided to the individual, records of correspondence relating to the request and a record of all decisions made relating to the request.

Further Guidance

Further guidance on subject access requests is available from the ICO website at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

SAR Process

Please follow the process below when responding to a subject access request.



Appendix 1: Template Subject Access Request Form

Please provide me with the information about me that I am entitled to under the General Data Protection Regulation and Data Protection Act 2018

Name	
Date of Request	
Relationship with the school	Please select: Pupil / parent / employee / governor / volunteer Other (please specify):
Correspondence address	
Contact number	
Email address	
Details of the information requested	Please provide me with: *Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example:* • *Your personnel file* • *Your child's medical records* • *Your child's behavior record, held by [insert class teacher]* • *Emails between 'A' and 'B' from [date]*

For School Use Only:

Date request received:	
Request received by:	
Request acknowledged:	
ID Verified – Item 1*	
ID Verified – Item 2*	
DPO informed date:	
Date information gathered:	
Date forwarded to DPO for authorisation:	
Headteacher approved:	
DPO approved:	

*The identity of the person making the request must be verified unless they are known to the school. Please record the type of ID and a reference number in these boxes.
Where the data subject is personally known (a staff member, for example), ID documents do not necessarily need to be provided. In this circumstance, 2 members of staff can sign to verify that the person is who they say they are.