EDSTART SCHOOLS

Internal SAR Procedures

INFORMATION GOVERNANCE

Policy owner	EdStart Specialist Education Ltd
Applies to	EdStart Schools – All Sites
Category	Information governance
Approval and validity	September 2026 to September 2027
Review trigger	Annual review, or earlier following statutory, regulatory or operational change

Status: This 2026 version supersedes all previous versions.

SUBJECT ACCESS INTERNAL PROCEDURES (SARS)

This Procedure is supplementary to the SAR Policy, and is not a substitute for it. This Procedure should be read in conjunction with the SAR Policy.

Introduction

1. This document is designed to provide an outline of the key points to consider when dealing with a SAR. It is not exhaustive and there will be situations that fall outside of this process. If this arises, the DPO will provide additional advice.

2. This is an internal facing procedure and is not for publication.

3. All those with responsibility for managing SARS should familiarise themselves with the ICO guidance in relation to SARS. (https://ico.org.uk/for-organisations/guide-to-data- protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right- of-access/) and have watched the HYin5ive training video on SARs.

STAGE 1 – Receiving and acknowledging the subject access request

Key objective is to make sure that the requester receives the information that they want.

4. The SAR should be sent to EdStart's dedicated data protection in box by emailing it to dataprotection@edstartschools.com 5. We will then triage the request, ensuring that it is a SAR. If it is, it will be forward to the DPO (DPO@wearehy.com).

6. The DPO will open a case file and assign a reference number to the request on Insight. The DPO will log all key dates on Insight so that the SAR is responded to in accordance with statutory timescales. The DPO will email EdStart confirming that these steps have been taken. Initial advice will be provided by the DPO as to the correct form of acknowledgment that needs to be sent.

7. When we receive a SAR, we need to aim to provide the requester with the information that they actually want, subject to any exemptions that may apply. Therefore, If the requester is asking generally for all personal data that the school holds about them, then we need to seek clarification to narrow down the request. This will assist both us

(as we do not want to review excessive amounts of personal data unnecessarily) and the data subject (who may not actually want all personal data that we hold). If we need to ask for further clarification, then the time for responding does not start until clarification is provided. If the request needs to be clarified – use Standard Template HY1. If the requester does not respond, then we will need to determine the extent to which we comply with the request.

8. If the request is reasonable and no clarification is required – use Standard Template HY2.

9. If for some reason we are not satisfied or unsure that the person requesting the personal data is who they say they are then identification should be requested – use Standard Template HY3.

10. Remember, if a parent requests their child's data, it is the child's data not the parent's.

STAGE 2 – Locating the data

Key objective is to ensure reasonable searches are undertaken to identify personal information relevant to the request

11. The DPO will arrange a meeting with EdStart to discuss the request.

12. EdStart will agree the searches that should be made with the DPO.

13. EdStart will undertake the searches and collate the personal data identified as relevant to the request.

STAGE 3 – Reviewing the request

Key objective is to review the request in a reasonable and proportionate manner.

14. Once personal data has been identified, it must be reviewed to identify any personal information that either requires (a) redaction or (b) is exempt from disclosure.

15. The DPO will provide any additional guidance required regarding redactions or the application of exemptions on request from EdStart.

16. Once the review has been completed, prepare Standard Template HY5 if the request relates to pupils and Standard Template HY6 if the request is from a staff member.

Exemptions

17. There are various exemptions which may be applied which means that personal data is exempt from disclosure. The more common exemptions we are likely to apply are listed below:-

Communications such as emails between

- Legal professional privilege the school and legal advisors are not to be disclosed under any circumstances. Safeguarding personal data Safeguarding personal data must be handled with caution. If disclosure is likely to cause physical or mental harm to the child, it must not be disclosed. In these circumstances, apply the serious harm test – use Standard Template HY8 to keep a record of our decision. This must be

signed off by the DPO. Employer references References provided by employers about ex-employees are exempt from disclosure.

Common scenarios

This section of the procedure is 'live' and should be added to on an ongoing basis where specific problems are encountered to ensure consistency in responding.

Topic Area Scenario Answer

What is classed as What if the data subject is An email may reference an identifiable individual (e.g. personal data? copied into an email, but their personal email address) but not be personal data none of the data contained about that individual – there must be something in the in the email relates to email which relates to them as well. them? The basic test to be applied is as follows:-

- If the information directly relates to the individual, then it should be disclosed.
- If the information is not at all related to them e.g. they are copied into an email about someone else, then this is not disclosable
- There are likely to be grey areas. However, as a general rule, if the data does in some way impact upon the data subject, it should be disclosed. If in doubt, it is good practice to disclose.

Third party data What if the personal data • Where disclosure means revealing personal contains data about other data concerning another child, then apply people? redactions to protect their identity. However, even if another child's name is redacted, you must consider whether the receiver of the data would still be able to identify that child. If they would, then we must not disclose (at least not without consent of the third party). As an example, if there was a fight in the playground and a parent asked for a copy of the behaviour log, it may be that no amount of redaction will protect the identity of the other children.

- We generally do not redact the names of teachers when a parent makes a SAR. However, there may be circumstances when a teacher may be entitled to confidentiality. If communications by a teacher are in relation to a child's behaviour, or the teacher gives opinions or makes observations, they are likely to not require redactions. However, if (as an example) a teacher confidentially makes a complaint about another teacher, then they are likely to expect a degree of confidentiality, and this

should be redacted (or the teacher's consent obtained).