Subject Access Request (SAR) Policy

Whole School & EYFS

Regulation ISSR:
Reviewed and updated by: MR
Approval: Full Governor Board
Last Review: Autumn 2024
Next Review: Autumn 2025

ALDERLEY EDGE SCHOOL FOR GIRLS

1. Introduction

The General Data Protection Regulation and Data Protection Act 2018 (hereinafter called the data protection laws) detail rights of access to both manual data (which is recorded in a relevant filing system) and computer data for the data subject. This is known as a Data Subject Access Request (SAR).

This right, commonly referred to as subject access, is created by Article 15 of the GDPR. It is most often used by individuals who want to see a copy of the information an organisation holds about them. However, the right of access goes further than this, and an individual who makes a written request is entitled to be:

- told whether any personal data is being processed;
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- given a copy of the information comprising the data; and given details of the source of the data (where this is available).

Under the data protection laws, organisations are required to have policies/procedures in place to ensure that individuals' rights of access are met within a timely and appropriate manner and seek to enable all who wish to do so to have access to the records that are held about them.

2. Compliance with the UK GDPR and Data Protection Act 2018

Under the data protection laws, organisations are required to respond to subject access requests within 1 month of receiving the request, or in the case of complex requests, within 3 months of receiving the request. Failure to do so is a breach of the Act and could lead to a complaint being made to the Information Commissioner's Office (ICO).

To assist the obligation to provide information within the time limits, the School will ensure that all employees are aware of how a subject access request should be made and of the requirement to respond to requests quickly.

The Data Protection Lead for the School will seek technical and legal advice on any complex requests as appropriate.

3. Aim

This Policy details how the School will meet its legal obligations concerning individual's access to their information. The requirements within the Procedure are based upon the data protection laws.

This Policy has been written to ensure that all staff are aware of their responsibilities to provide information if requested.

4. Legislation

For the purpose of this Policy other relevant legislation and appropriate guidance may be referenced. The legislations listed below also refer to issues of security of personal confidential data:

- Regulation of Investigatory Powers Act 2000
- Crime and Disorder Act 1998
- Computer Misuse Act 1990
- Criminal Justice and Immigration Act 2008
- Health and Social Care Act 2012

Any request for access to medical records will be processed in line with the Access to Health Records Act 1990.

Where individuals are applying for access to a deceased person's records the Access to Health Records Act 1990 will be followed.

Health records relating to deceased person will be treated with the same level of confidentiality as those relating to living people. Under the Access to Health Records Act 1990 a request to see a deceased person's health record or to have a copy thereof can be made by the personal representative or any person who may have a claim arising out of the person's death.

The personal representative (executor or next of kin – who may be a relative, friend or solicitor) or anyone having a claim resulting from the death has the right to apply for access to the relevant part(s) of the deceased's health record under the 'Access to Health Records Act 1990'. Where the requestor is not acting in a legal capacity, they should detail why they need access in pursuing a claim. Where they are the executor or administrator, they must provide proof of appointment under the Will/Grant of probate

5. Related Guidance

The following are the main publications referring to security and or confidentiality of personal sensitive data:

- Information Commissioner's Office: Subject Access Request Code of Practice

6. Roles and Responsibilities

6.1 Accountable Officer

The Chair of governors has overall responsibility for the Data Subject Access Policy. The Chair of Governors has delegated SAR operational responsibilities to the School's Data Protection Lead.

6.2 Data Protection Lead

The Data Protection Lead is responsible for ensuring that SARs are effectively coordinated, managed and procedures are in place to support access to records, including:

- Reviewing Subject Access Requests
- Ensuring that requests are actioned by fully trained and resourced staff
- All staff members are aware of the need to support subject access requests, and where in the organisation such requests should be directed.

The School's Data Protection lead has responsibility for ensuring compliance issues are brought to the attention of the Governing Body.

6.3 All Staff

All staff should ensure that:

- They are aware of their responsibility to support subject access requests and they must notify the School's Data Protection Lead without delay
- they comply with this SAR Policy and all related policies and procedures
- personal sensitive data and records (whether in electronic or manual) relating to pupils and staff are kept secure, accurate, relevant and up to date.

Members of staff who would like access to their personal confidential/sensitive information must submit their requests in writing to the School's Data Protection Lead – mrigby@aesg.co.uk.

7. Training

The School will ensure all permanent/temporary/contract staff complete online training as part of the induction process, with further training required for, staff who process SARs.

8. Dissemination and Implementation

This Policy will be publicised on the School's Intranet. Line Managers are required to ensure that their staff understand its application. Awareness of any new content/change in process will be through staff briefing in the first instance. Where a substantive revision is made, then a separate plan for communicating and implementing this change will be devised .

9. Monitoring & Audit

This Policy will be monitored by the Governing Board to ensure any legislative changes that occur are incorporated in the document. The Policy will be reviewed regularly by the Data Protection Lead, which may necessitate an earlier review, if there has been changes to legislation.

The process for dealing with Data Subject Access requests for personal information held by Alderley Edge School for Girls are outlined in the Appendices attached.

Appendix 1: How AESG process SARs

When a subject access request is received it should immediately be reported to the Data Protection Lead, who will then coordinate the response. Teams may be required to provide information relating to this request.

It should be noted that individuals have a right under data protection laws to:

- know whether their personal information is being processed (which includes being held or stored)
- be given a description of the data held, the purpose for which it is processed and to whom the data may be disclosed.
- be given a copy of the information held.
- be given information as to the source of the data

If a request has already been complied with and an identical or similar request is received from the same individual there is no obligation to comply with the second request unless a reasonable interval has elapsed.

Requests should include the full name and address of the person seeking access to their information. To comply with the Act, information relating to the individual must only be disclosed once identity has been confirmed.

The School is required to record all incoming requests for information and track them through to completion. The Data Protection Lead will acknowledge all requests for information and record the key dates and information relating to the request in a central register.

Identity

Adequate steps will be taken to identify the requester. Examples of suitable documentation are:

- Valid Passport
- Driving Licence
- Birth Certificate along with some other proof of address e.g. a named utility bill (no longer than 3 months old) or a Medical Card.
- Information that is only known to the organisation and subject.

Methods of identity confirmation will not exceed the level of personal data held by the School.

Fees

There will be no charge for subject access requests unless they are unfounded or excessive and then the School reserves the right to charge on a request-by-request basis but at a reasonable rate.

Authorisation of a child over 12 years old.

Under the Data Protection Act the school is required to consider the data protection rights of any child over the age of 12 with the competence to understand their actions. If it is

determined that a child is competent, the organisation should allow a parent to exercise rights, including the right of access, only if the child authorises them to do so, unless it is in the child best interests.

If a pupil wishes to withhold authorisation it is important that some form of assessment of competence is carried out which would be along the same line as a Ghilick assessment, that is…

"the pupil understands the implications of providing or withholding their consent and has not conducted any other action which would demonstrate a lack of competence.".

Please ensure a paper trail of the conversation to establish competence, this could be via email, in case of challenge by a parent or guardian.

Once competence has been established an email should be sent to the Date Protection Lead…

"it is the professional opinion of the School that the pupil is competent to exercise their rights and the School is not aware of any grounds to overrule their wishes and authorise the sharing in their best interests".

Subject access requests made on behalf of people who lack capacity

If an adult lacks capacity and a representative is making the request on their behalf, the person dealing with the request must satisfy themselves that the request is being made in the individual's best interest.

Deadlines

A request is required to be fulfilled within one month unless the request is complex and then it is required to be fulfilled within three months, but without undue delay.
Examples of complex requests provided by the ICO include:

- technical difficulties in retrieving data (e.g. where data is electronically archived);
- the request involves large volumes of sensitive data (as more time would be required to consider redactions);
- clarify potential issues around disclosing information of a child to a guardian (i.e. where evidence of a guardianship order has not yet been provided); and
- specialist work to redact or communicate (i.e. editing an audio or video file before release).

It is understood that it will be difficult to establish the extent of information prior to conducting the search but a useful example could be if a parent requests all information for a student who has been with the school since the beginning of phase with extensive SEND or safeguarding issues, then it would be reasonable to assume that the request would be complex.

If a request is determined to be complex then the requester must be notified of the extended timeline for disclosure, within the first month.

What information should be provided?

All information, which relates to the data subject, should be provided subject to any data protection exemptions that may apply, for example information provided by third parties, as part of a confidential reference, part of management planning, given in confidence, or information that may cause harm or distress to the data subject or others, if disclosed.

Where the record contains the personal information on more than one person, consideration should be given to the interests of all the parties before deciding whether or not you may disclose the information.

Information must be supplied to the individual in permanent form, if requested, unless to do so would involve 'disproportionate' effort. For manual records this would involve photocopies. For computerised records these can be supplied in electronic format but must contain explanations of codes or abbreviations where appropriate. If the 'disproportionate' effort issue arises, the records can be shared with the individual on a face-to-face basis who can be asked to visit the premises to view their records.

Original records must not be released because of the potential detriment to the individual should the records be lost. Copies must always be provided.

Conducting a search for data

A requester is not entitled to "everything where my name is mentioned", instead they are entitled to information that relates to them or their child. The ICO defines "relates" as:

1/ The context is clearly about the data subject i.e. they are the topic of conversation.

2/ The purpose is to evaluate the subject i.e. treat them in a certain way or influence their status or behavior.

3/ The result has an impact on the subject i.e. the records operation of equipment which the subject's salary or bonus is aligned to.

If we take a telephone list, it is not about a single subject, it does not evaluate any of the subjects or influence their status or behavior or have any effect or impact on them.

If we take emails, a request does **not** cover every email where the subject is in the To, CC or BCC, instead, it is only where their name appears in the subject line or body of the text as only then are they the topic of conversation, i.e. it is clearly about them.

Redaction(s):

Information can be withheld(redacted). in part, or in full, if it meets one of the following exemptions:

- legal or professional privilege – conversations with school/trust legal counsel or school counsellor;
- reference given in confidence for employment, training, volunteering or educational purposes;
- processed for the purpose of management planning – conversations on staffing levels etc.;
- consists of records of intentions in relation to negotiations between employer/employee;

- contains the personal data of a third party – unless the requester would reasonably know it; or
- likely to prejudice the prevention or detection of a crime – information provided to the police.

Important: Please remember, the exemption for confidential references only covers the reference itself and does not cover other records or communications which may discuss the reference.

Important: Even if the personal data is not labelled confidential or processed as part of a recognised confidential activity, it could be considered to be confidential under common law.

Important: Ensure an unredacted copy of all disclosed information is securely retained in case of challenge.

Complaints

If an individual is dissatisfied with the way their subject access request has been managed, they should be advised to invoke the School's complaint process. If they are still dissatisfied, they can complain to the Information Commissioner's Office. This can be done in writing to:
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5A