



# SUBJECT ACCESS REQUEST POLICY

**This policy is reviewed every three years by the Trust Board**

## History of Document

Issue No	Author/Owner	Date Written	Approved by Trust Board	Comments
1	DPO	June 2018	12 July 2018	1 <sup>st</sup> formal issue
2	DPO	Dec 2018	13 December 2018	Removal 4.4 Minor amendment to 5.3
3	DPO	February 2019	14 February 2019	Minor amendments from ICO audit
4	DPO	December 2019	12 December 2019	Minor amendment 10.1
5	DPO	December 2021	9 December 2021	Changes to sections 5,6,7 9,

## 1. INTRODUCTION

- 1.1 The Active Learning Trust (“Trust”) collects, uses, shares, reports, retains, processes and deletes/destroys personal information about students, staff, parents or carers, and other individuals who come into contact with the Trust. This information is gathered to enable the Trust to provide education and other associated functions in relation to its employment of staff and duty of care to young people. In addition, there may be a legal requirement to collect and use information to ensure that the Trust complies with its statutory obligations.
- 1.2 Data protection legislation gives individuals (“data subjects”) the right of access, (commonly referred to as subject access) to obtain a copy of their personal data that an organisation holds about them. When an individual makes a request to view their information it is known as a Subject Access Request (“SAR”).
- 1.3 It is important that all members of staff are able to recognise that any request made by a person for their own information or that of a different person, the data subject, is likely to be a valid subject access request, even if the individual doesn’t specifically use this phrase in their request or refer to the UK GDPR. In some cases, an individual may mistakenly refer to the “Freedom of Information Act” but this should not prevent a school from identifying the request as being made under the UK GDPR if appropriate. Some requests may be a combination of a subject access request for personal data under the UK GDPR and a request for information under the Freedom of Information Act.

## 2. PURPOSE OF THE POLICY

- 2.1 The purpose of the Trust’s Subject Access Request Policy (“Policy”) is to outline the framework for receiving and responding to a SAR.
- 2.2 This Policy is based on the Information Commissioner’s Office (ICO) Right of access guidance [Link](#)

## 3. SCOPE

- 3.1 This Policy is intended for anyone who submits SARs to the Trust or responds to SARs on behalf of the Trust.
- 3.2 Personal data is information that identifies an individual and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain<sup>1</sup> such as a name, date of birth,

---

<sup>1</sup> For example, if asked for the number of female employees, and you only have one female employee, this would be personal data if it was possible to obtain a list of employees from the website.

address, NI number, medical information, exam results and an online identifier, such as an IP address. A sub-set of personal data is known as special category personal data. This special category data is information that reveals:

- 3.2.1 race or ethnic origin;
- 3.2.2 political opinions;
- 3.2.3 religious or philosophical beliefs;
- 3.2.4 trade union membership;
- 3.2.5 physical or mental health;
- 3.2.6 an individual's sex life or sexual orientation;
- 3.2.7 genetic or biometric data for the purpose of uniquely identifying a natural person

#### **4. RESPONSIBILITIES**

- 4.1 The Trust Board has ultimate responsibility for setting this Policy.
- 4.2 A Headteacher is responsible for ensuring that the requirements relating to this Policy are adopted and adhered to and is responsible for the day to day management of SAR arrangements. Where the term Headteacher is used this incorporates Executive Headteacher roles where these exist and the Chief Executive Officer of the Active Learning Trust when the statement refers to the Central Team.
- 4.3 If employees e.g. teachers are contacted directly by a parent/carer/child e.g. in the playground at the end of the school day, for their personal data or that of their child held by the school, they should advise the individual to contact the school's Headteacher or Business Manager directly on such matter. They must not provide personal data outside the Trust's agreed policy for processing subject access requests. All subject access requests must be processed by a school's Headteacher or Business Manager in accordance with this Policy and the Trust's written procedures.
- 4.4 The Trust's Data Protection Officer ("DPO") submits a report on the effectiveness of the Policy to the Trust Board as a minimum on an annual basis.
- 4.5 Everyone who processes subject access requests must comply with this Policy.

## **5. IDENTIFYING A SUBJECT ACCESS**

- 5.1 A request does not need to include the phrases “subject access request”, “right of access” or “Article 15 of the UK GDPR”. A request may be a valid SAR even if it refers to other legislation, such as the Freedom of Information Act 2000 (FOIA). It just needs to be clear that the individual is asking for a copy of personal data held.
- 5.2 Routine verbal enquiries and correspondence that are routinely dealt with in the normal course of business and can be responded to quickly are not SARs. The SAR process may be appropriate where an individual requests a high volume of information and there is a need to conduct a time-consuming search of records in order to comply with the request. For example, if an individual requests copies of letters which have been sent to them previously, it is unlikely that this should be dealt with as a formal SAR. Schools must consider these enquiries on a case by case basis.

## **6. FORMAT OF REQUESTS**

- 6.1 An individual can make a SAR verbally or in writing, including on social media channels. Completion of the Trust’s SAR form is the Trust’s preferred method. A copy of the SAR form is held on both the Trust’s and schools’ websites. The SAR form is also available in hard copy format from a school’s reception.
- 6.2 Guidance has been produced how to complete the Trust’s SAR form (refer Appendix I).

## **7. SAR RECEIPT**

- 7.1 All SARs should be sent to a school’s Headteacher with a copy sent securely to the Trust’s DPO who will arrange for it to be recorded in the Trust’s SAR Log and a reference number issued.
- 7.2 An acknowledgement email or letter will be sent to an individual by the school or the Trust’s DPO which includes the reference number.
- 7.3 If a request relates to both the requester’s personal data and to other information, this should be treated this as two requests:
- one for the requester’s personal data, made under the UK GDPR; and
  - another for the remaining information, made under FOIA or the EIR

It is important to consider the requested information under the right legislation. This is because a disclosure under FOIA or the EIR is to the world at large – not just the requester. If personal data is mistakenly disclosed under FOIA or the EIR, this could lead to a personal data breach.

## **8. IDENTIFICATION**

- 8.1 Two forms of identification may be requested to check that personal information is being provided to the correct individual at the correct address. This however isn't always necessary as a staff member may be able to verify the identity of the data subject/requestor. If there is uncertainty about the identity of the individual making the SAR, then additional information may be requested to confirm the individual's identity.
- 8.2 The timescale for responding to a SAR does not begin until the school has received the requested information. However, schools should request ID documents promptly.
- 8.3 Any individual, including a child or young person with ownership of their own information rights, may appoint another person to request access to their personal data. In such circumstances the Trust must have written evidence that the individual has authorised and provided consent for the person to make the application and the Headteacher must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

## **8. REQUESTS FOR LARGE AMOUNTS OF PERSONAL DATA**

- 7.1 Individuals may be asked to clarify the information that a request relates to, if a large quantity of information is processed about an individual, so that the information supplied, is relevant.

## **9. FEES**

- 8.1 No fee will be charged for responding to SARs. However, if many requests are received for the same personal data from the same individual, data protection legislation allows the Trust to charge a reasonable fee based on the administrative cost of providing the information. Individuals will be informed of such charge prior to the personal data being obtained.

## **9. REFUSING TO RESPOND TO A SAR**

- 9.1 Where an exemption applies, a school may refuse to provide all or some of the requested information, depending on the circumstances.

- 9.2 Per UK GDPR Article 12 (5) (b) a school can refuse to comply with a SAR if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.
- 9.3 A request may be manifestly unfounded if:
- the individual clearly has no intention to exercise their right of access. For example an individual makes a request, but then offers to withdraw it in return for some form of benefit from the organisation; or
  - the request is malicious in intent and is being used to harass an organisation with no real purpose other than to cause disruption. For example, the individual:
    - explicitly states, in the request itself or in other communications, that they intend to cause disruption;
    - makes unsubstantiated accusations against you or specific employees which are clearly prompted by malice;
    - targets a particular employee against whom they have some personal grudge; or
    - systematically sends different requests to you as part of a campaign, e.g. once a week, with the intention of causing disruption.
- 9.4 A request may be deemed manifestly excessive if it is deemed unproportionate when balanced with the burden or costs involved in dealing with the request. This will mean taking into account all the circumstances of the request, including:
- the nature of the requested information;
  - the context of the request, and the relationship between the school and the individual;
  - whether a refusal to provide the information or even acknowledge if a school holds it may cause substantive damage to the individual;
  - a school's available resources;
  - whether the request largely repeats previous requests and a reasonable interval hasn't elapsed; or
  - whether it overlaps with other requests (although if it relates to a completely separate set of information it is unlikely to be excessive).
- 9.5 A request is not necessarily excessive just because the individual requests a large amount of information. Schools must consider all the circumstances of the request. Schools should also consider asking the individual for more information to help them locate the information they want and whether the school can make reasonable searches for the information. Refer 'Can we clarify the request?' and 'What efforts should we make to find information?'.

9.6 Schools should consider the following when deciding whether a reasonable interval has elapsed:

- the nature of the data – this could include whether it is particularly sensitive; and
- how often a school alters the data – if it's unlikely that the information has changed between requests, a school may decide not to respond to the same request twice. However, if a school has deleted information since the last request, it should inform the individual of this.

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

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

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

9.8 If a school refuses to comply with a request, it must inform the individual of

- the reasons why;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through the courts.

## **10. RESPONSE TIMEFRAME**

10.1 Responses to SARs will be provided without undue delay and at the latest within one month of receiving the request with the day of receipt counting as 'day one' e.g. a SAR received on 3 September should be responded to by 3 October.

10.2 Reasonable efforts should be made to find and retrieve the requested information. However, schools are not required to conduct searches that would be unreasonable or disproportionate to the importance of providing access to the information. To determine whether searches may be unreasonable or disproportionate, schools must consider:

- the circumstances of the request;
- any difficulties involved in finding the information; and
- the fundamental nature of the right of access.

The burden of proof is on schools to be able to justify why a search is unreasonable or disproportionate.

- 10.3 The timeframe to respond to a SAR can be extended by a further two months if the request is complex (e.g. those that require a high volume of material or require additional steps to process, such as the need to search for records in multiple locations) or a school has received numerous requests from the same individual e.g. other types of requests relating to individuals' rights. The Trust's DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period. If this is the case, an individual must be informed in writing within one month of the receipt of the request with an explanation why the extension is necessary. Where an extension is required, information will be provided within three months of the request.
- 10.4 It is the ICO's view that it is unlikely to be reasonable to extend the time limit if:
- it is manifestly unfounded or excessive;
  - an exemption applies; or
  - a school is requesting proof of identity before considering the request.
- 10.5 Individuals will be made aware that it may be harder to access personal information and respond during summer holidays. Where possible SARs should be sent to the Trust's Data Protection Officer at [dataprotection@activelearningtrust.org](mailto:dataprotection@activelearningtrust.org) during the summer holidays so their receipt can be acknowledged.
- 10.6 The one-month time limit can't be extended on the basis that a school has to rely on a processor to provide the information that is needed in a response.
- 10.7 Where the issue of a response requires to be extended from one month to three, the DPO will escalate such issue to the Director of Finance and Operations and comment on any delays in the DPO's Information Governance Report to the Trust Board.
- 10.8 If a school processes a large amount of information about an individual, it may be able to ask the requestor to specify the information or processing activities their request relates to, if it is not clear. The time limit for responding to the request is paused until a school receives clarification, although the school should supply any of the supplementary information it can within one month.

## **11. SHARING PERSONAL DATA WITH THIRD PARTIES**

- 11.1 A data subject can ask a school to share his/her personal information with another person such as an appointed representative e.g. relative, friend or solicitor. In such cases a school should request written authorisation signed by the data subject, confirming which of his/her personal data they would like a school to share with the other person.



- 11.2 If a request is made by a third party seeking the personal data of the data subject (e.g. relative, friend or a solicitor acting on behalf of a client), a school needs to be satisfied that the third party making the request is entitled to act on behalf of the individual. 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 school should not contact the data subject directly for such evidence.
- 11.3 If a school 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.
- 11.4 Consent to disclose a data subject's personal data to a third party is only valid if such consent is freely given so if a school considers that a person has been coerced to provide consent for their personal data to be disclosed to the requestor, then it is not valid consent. If there is no valid consent, then there is no SAR and in such situation a school will have to consider what information it could voluntarily provide to the requestor in the absence of any consent from the data subject.
- 11.5 If a requestor has sought and obtained consent from the data subject for the release of a data subject's personal data but not their own, then any personal data relating purely to the requestor may be removed as falling outside the scope of the request. However, schools may find that the requestor comes back at a later date and makes a subject access request for their own personal data.
- 11.6 Where a school has personal data relating to both the requestor and data subject then a school will need to apply the rule about third party data. An example of where a school may have mixed personal data is that between a parent and student where the parent passes an opinion about the student. This is the parent's opinion which is the parent's personal data but it is information which relates to the student so it is also the student's personal data.
- 11.7 The application of the third party data rule means that a school can only disclose the parent's personal data if it is reasonable to do so or if a school has the parent's consent. It is important to remember that the request is treated as the student's subject access request, if the student has provided consent to disclosure and the law assumes that the student will see the disclosure.
- 11.8 As far as the third party data rule goes it is the same for any third party so it does not take into account that the material is actually being disclosed to the parent. If a school does not think it is reasonable to disclose a parent's personal data to their child (and a school does not have the parent's consent to the disclosure) then it can be removed. In deciding what is reasonable, a school must by law have regard to all the relevant circumstances including the following matters:
- the type and nature of information that a school would disclose;
  - any duty of confidentiality the school owes to the requestor and/or child;

- any steps the school has taken to seek consent from the requestor;
- whether the requestor is capable of giving consent; and
- any express refusal of consent by the requestor;
- where possible the child's level of maturity and their ability to make decisions like this;
- any court orders relating to parental access or responsibility that may apply;
- any consequences of allowing those with parental responsibility access to the child's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child if individuals with parental responsibility can't access this information;
- any views the pupil has on whether their parents or carers should have access to information about them.

11.9 The decision to disclose personal data will therefore involve balancing the data subject's right of access against the other individual's rights.

## **12. REQUESTS MADE ON BEHALF OF CHILDREN**

12.1 A child's personal data belongs to a child irrespective of their age. The rights in relation to that personal data are theirs and not those of their parents/carers even if

- they are too young to understand the implications of the right of access;
- the right is exercised by those who have parental responsibility for the child; or
- they have authorised another person to exercise the right on their behalf.

12.2 Primary Schools – Children below the age of 12 are not generally considered mature enough to understand their rights and implications of a SAR. Therefore most SARs from parents or carers of primary school aged children may be granted without the express permission of the pupil.

12.3 Secondary Schools - Children aged 12 and above are generally considered mature enough to understand their rights and implications of a SAR. Therefore most SARs from parents or carers may not be granted without the express permission/consent of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case by case basis.

12.4 When considering subject access requests, the points outlined in 11.8 above should be taken into account

### **13. REQUESTS IN RESPECT OF CRIME AND TAXATION (e.g. POLICE or HMRC) – SCHEDULE 2 PART 1 PARA 2 DPA 2018**

13.1 Requests for personal information may be made by the above authorities for the following purposes:

- The prevention or detection of crime
- The capture or prosecution of offenders
- The assessment or collection of tax or duty

13.2 A formal documented request signed by a senior officer from the relevant authority is required before proceeding with the SAR. The SAR must make it clear that one of the above purposes is being investigated and that not receiving the information would prejudice the investigation. These types of requests must be considered by the Trust's DPO.

13.3 Schools are not legally obliged to provide the information.

13.4 The data subject must not be informed of the request as to do so is likely to prejudice the matters raised in the request.

### **14. COURT ORDERS**

14.1 Any Court Order requiring the supply of personal information must be complied with.

### **15. REDACTION OF INFORMATION**

15.1 An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

15.2 If documents with personal data includes information about someone else, such information will be redacted (information blacked out/removed) before supplying the personal data to the requestor or the Trust may decline to provide it, if disclosing it would 'adversely affect the rights and freedoms of others.' The Trust has issued "How to Redact/Blank Out Guidance" to assist with this task. The Trust will also refer to the ICO's guidance "How to disclose information safely - removing personal data from information requests and datasets - [Guidance](#)

15.3 Where redaction has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what information was redacted and why.

- 15.4 Where all the data in a document cannot be disclosed, a permanent copy should be made, and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.
- 15.5 Before disclosing third party information i.e. that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school, consent should normally be obtained.
- 15.6 A second person authorised by a Headteacher is required to check that all necessary redactions have been made before disclosure in cases where the DPO has not undertaken the redaction.
- 15.7 All draft SAR responses and redacted documentation must be sent securely to the Trust's DPO for review prior to their issue by a school to a requestor, unless the Trust's DPO has undertaken the redaction and determined whether any exemptions are to be applied.

## **16. PROTECTION OF THIRD PARTIES – EXEMPTIONS TO THE RIGHT OF SUBJECT ACCESS**

- 16.1 The UK GDPR and the Data Protection Act 2018 set out exemptions from some of the rights and obligations in some circumstances. Exemptions should not routinely be relied upon and should be considered on a case-by-case basis. The main ones which are detailed in the Trust's SAR guidance and apply to schools are:
- Confidential references – prospective or actual regardless of whether a Data Controller has given or received a reference.
  - Negotiations between Employer and Employee - the release of the data would prejudice the negotiations
  - Management Forecasting/planning - and its release to an individual would prejudice the conduct of the Trust's business or activities
  - Complaints
  - Legal professional privilege
  - Exam Scripts and Marks —Candidates do not have the right to copies of their answers to the exam questions. The information recorded by the person marking the exam is not exempt. However, if an individual makes a SAR for this information before the results are announced, special rules apply to how long schools have to comply with the request. Schools must provide the information within:

- five months of receiving the request; or
- 40 days of announcing the exam results, if this is earlier.

This excludes an examiner's comments.

- Preventing and Detecting crime – the release of the data would jeopardise the prevention or detection of crime, or the apprehension or prosecution of offenders
- Health Data - Serious Harm Test - safeguarding concerns may contain information about multiple children including siblings and estranged parents; files containing advice from doctors, police or probation services
- Education Data – Serious Harm
- Child Abuse Data - This includes physical injury (other than accidental injury) to, and physical and emotional neglect, ill-treatment and sexual abuse of, an individual aged under 18. Safeguarding concerns may contain information about multiple children including siblings and estranged parents; files containing advice from doctors, police or probation services.

Schools are exempt from providing child abuse data in response to a SAR if it receives a request (in exercise of a power conferred by an enactment or rule of law) from someone:

- with parental responsibility for an individual aged under 18; or
- appointed by a court to manage the affairs of an individual who is incapable of managing their own affairs.

But the exemption only applies to the extent that complying with the request would not be in the best interests of the child.

16.2 Where personal data is not to be provided due to application of an exemption, a school should ensure it internally documents its reasoning for withholding this data. The personal data withheld and exemption applied should also be recorded in the Trust's SAR Log by the Trust's DPO.

## 17. SAR RESPONSE

17.1 In addition to a copy of the personal data, the requestor must be provided with the following supplemental information much of which may already be supplied in a school's privacy notice:

- the purposes of the school's processing;
- the categories of personal data concerned;

- the recipients or categories of recipient that the school discloses the personal data to;
- the school's retention period for storing the personal data or, where this is not possible, the school's criteria for determining how long it will store it
- the existence of their right to request rectification, erasure or restriction or to object to such processing;
- the right to lodge a complaint with the ICO or another supervisory authority;
- information about the source of the data, where it was not obtained directly from the individual;
- whether the school undertakes any automated decision-making (including profiling); and
- the safeguards the school provides if it transfers personal data to a third country or international organisation.

17.2 SAR responses and redacted documentation may be provided to the requestor at school with a member of staff on hand to help and explain matters if requested, sent by secure email or sent by recorded post.

17.3 Schools may require the requestor to sign and return a copy of the covering letter issued with the documents by way of confirming receipt of the documentation.

## **18. RETENTION**

18.1 SARs and responses will be retained in accordance with the Trust's Records Retention Policy.

18.2 The DPO will advise schools when the SAR documentation can be securely destroyed.

18.3 The bulk deletion log must record that the copy SAR information has been destroyed and such be authorised by a Headteacher.

## **19. MONITORING AND REPORTING**

19.1 The Trust's DPO will monitor the effectiveness of this Policy and relevant procedures as part of a Data Protection Annual Monitoring Programme.

19.2 All draft SAR responses and redacted documentation must be sent securely to the Trust's DPO for review prior to their issue by a school to a requestor.

19.3 Actual performance against SAR key performance indicators will be monitored by the Trust Board.

- 19.4 Formal cold case process for quality assessments and to check redactions are appropriate and exemptions are consistently applied, will be introduced when the Trust's DPO is not the person undertaking the redactions and applying the exemptions.

## 20. COMPLAINTS

- 20.1 If after a requestor has read the information a school has provided, they consider any of the following to be true, they should notify the Trust's Data Protection Officer at email: [dataprotection@activelearningtrust.org](mailto:dataprotection@activelearningtrust.org)
- the information is inaccurate or out of date;
  - the school should no longer be holding that information;
  - the school is using the personal information for a purpose of which the requester was not unaware;
  - the school may have passed inaccurate information about the data subject to someone else.
- 20.2 If the requester is not satisfied in any way about how their request has been answered they can complain using the Active Learning Trust's complaints policy which can be found on its website - [Link](#)
- 20.3 If following the conclusion of the complaints policy within the Active Learning Trust, the requester is still dissatisfied or the original decision is not reviewed, the requester can complain directly to the Information Commissioner's Office (ICO) at <https://ico.org.uk/concerns>
- 20.4 The Trust's DPO, once advised, will record any complaints and the nature of those complaints received by schools/Trust in relation to SARs and sent by requestors to the ICO, in the SAR Log and any subsequent action required. Complaints submitted to the ICO will be discussed with the Director of Operations and the Trust's Leadership Team and response agreed. The Trust's DPO reports on a complaints key performance indicator in the termly Information Governance report to the Trust Board – number of complaints expected/Trust aware of those that have been sent to the ICO re SAR responses.
- 20.5 If a complaint results in a requirement to make a change to the SAR Policy, the changes will be put to the Trust Board for consideration and approval and the revised Policy will be provided to all schools immediately thereafter. Any lessons learnt will be shared with schools in the subsequent Information Governance newsletter issued by the Trust's DPO. Should there be any amendments required to the Trust's Complaints Policy these will be undertaken by the Trust's Company Secretary.

## Appendix I



# SUBJECT ACCESS REQUEST (“SAR”) GUIDANCE

## How do I make a Subject Access Request?

Complete the SAR form and hand or email it to the School Office marked “**Subject Access Request.**” We will accept requests in other formats however this is our preferred method.

We may ask you to provide two forms of identification to check we are providing personal information to the correct person. This however isn’t always necessary and you could simply ask a staff member to verify your identity. If we are uncertain about the identity of the person making the SAR, then we are entitled to request additional information to confirm your identity.

## Requests for large amounts of personal data

We may ask you to specify the information the request relates to, if we process a large quantity of information about an individual, so that the information supplied, is relevant.

## Will I be charged for the information?

No. However if we receive many requests for the same personal data from the same individual we can charge a reasonable fee based on the administrative cost of providing the information. We would notify you of such charge prior to obtaining the personal data.

## What will I be advised?

We will write to you and confirm whether we hold any of your personal data and provide such copies.

We will also advise you of your rights for the personal data held which are recorded within a Privacy Notice.

## How long will it take?

We will contact you within a month. We can extend this period by a further two months where requests are complex (e.g. those that require a high volume of material or require additional steps to process such as the need to search for records in multiple locations). If this is the case, we will inform you within one month of the receipt of the request and explain why the extension is necessary.



**What action can the school take?**

If the personal data includes information about someone else, we will redact that information before supplying the personal data to you or we may decline to provide it, if disclosing it would 'adversely affect the rights and freedoms of others.' Where a request is made by email, the information will also be provided via email unless otherwise requested.



## SUBJECT ACCESS REQUEST FORM

PLEASE COMPLETE AND RETURN TO THE SCHOOL

### Section 1 – About you

<b>Title</b> <i>(please tick)</i>	<b>Mr</b>		<b>Mrs</b>		<b>Miss</b>		<b>Ms</b>		<b>Other</b>	
<b>Full Name</b>										
<b>Relationship with the School</b>	Please select – parent/carer, pupil, employee, governor, volunteer, other (please specify)									
<b>Current Address and Postcode</b>										
<b>Telephone Number</b>										
<b>Email Address</b>										
<b>Preferred method of response – email or hard copy (for collection from the school office)</b>										

### Section 2 – What information are you requesting?

Please describe the personal information you are requesting
---

**Section 3 – Proof of Identity (IF REQUIRED)**

Please provide copies of two pieces of identification, one from list A and one from list B below for yourself and indicate which ones you are supplying. These will be securely destroyed after the SAR has been responded to. If we are not satisfied you are who you claim to be, we reserve the right to refuse to grant your request.

**Please DO NOT send any original documents**

**List A (photocopy of one from below)**

**List B (photocopy of one from below)**

Passport	<input type="checkbox"/>	Utility bill showing current home address	<input type="checkbox"/>
Photo driving licence	<input type="checkbox"/>	Credit card statement (no more than 3 months old)	<input type="checkbox"/>
Foreign National Identity Card	<input type="checkbox"/>	Bank statement or Building Society Book	<input type="checkbox"/>
Birth Certificate	<input type="checkbox"/>	Local authority tax bill	<input type="checkbox"/>

**Section 4– Signature**

<b>Signature</b>		<b>Date</b>	
------------------	--	-------------	--

If after you have received the information you have requested, you believe that:

- the information is inaccurate or out of date; or
- we should no longer be holding that information; or
- we are using your information for a purpose of which you were unaware; or
- we may have passed inaccurate information about you to someone else.

**PLEASE** notify the Trust’s Data Protection Officer – email [dataprotection@activelearningtrust.org](mailto:dataprotection@activelearningtrust.org)