SOLENT
Academies Trust

Together we inspire lifelong learning, perseverance, kindness and growth, transforming the lives of our children and families

SUBJECT ACCESS REQUEST POLICY

Scope:	Trust Policy
Author:	Data Protection Officer
Name of Responsible Officer:	Data Protection Officer
Approving Committee:	Chief Finance and Operations Officer
Statutory Basis:	Statutory Policy
Requirement to publish on website:	Yes – Trust and all Academies
Date ratified by approving committee:	October 2024
Review Period:	Bi Annually
Review date:	October 2026

Company Registration No:08374351, Solent Academies Trust is a Charity and a Limited Company

Contents

1. Introduction and Purpose 3
2. Policy Statement 3
3. Scope of the Policy 3
4. Key Definitions 4
5. Duties of the Information Commissioners Office 5
6. Roles and Responsibilities 5
7. How can an individual make a Subject Access Request? 6
8. Can individuals request personal information on behalf of another person? 6
9. How long do we have to respond? 7
10. Can I charge for the request? 7
11. What do I do if I receive a request? 7
12. How do I locate the information requested? 7
13. Can I provide all information found relating to the data subject? 7
14. What is a double check? 8
15. How do I respond to a Subject Access Request? 8
16. Complaints 8

16.2. Complaining to the Information Commissioners Office 9

1. Introduction and Purpose

The Data Protection Act 2018 (the Act) gives individuals rights of access to their personal records held by Solent Academies Trust. Subject access is a fundamental right for individuals, but it is also an opportunity for the trust to provide excellent customer service by responding to Subject Access Requests (SARs) efficiently and transparently and by maximising the quality of the personal information you hold. This Policy explains how the trust will fulfil its obligations under the Act.

2.Policy Statement

Solent Academies Trust regards the Act as an important mechanism in achieving an honest, safe and open relationship with its students and employees.

Subject access is most often used by individuals who want to see a copy of the information the trust holds about them. However, subject access goes further than this and an individual 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 personal data; and
- Given details of the source of the data (where this is available).

An individual can also request information about the reasoning behind any automated decisions taken about him or her, such as a computer-generated decision for benefit or a grant entitlement, or an assessment of performance at work.

The aim of this policy is to ensure that the trust complies with its legal obligations under the Data Protection Act 2018 and can evidence that you have done so. It also aims to ensure that you:

- Have robust processes in place for dealing with subject assess requests, saving time and effort;
- Increase levels of trust and confidence by being open with individuals about the personal information you hold;
- Improve the transparency of your activities in line with public policy requirements.

This policy should be read in conjunction with the Subject Access Request Procedure.

3.Scope of the Policy

This document outlines how an applicant can make a request for their personal information under the Act and how it will be processed.

This is not a legal document. It does not confer rights nor override any legal or statutory provisions which either require or prevent disclosure of personal information.

This document takes into account the key features of the Act and outlines how the trust will take steps to ensure compliance in relation to requests for personal information.

Requests for access to the records of people who are deceased are not within scope of this

Policy as the Act only applies to the data of living individuals. Such requests will be treated as requests for access to information under the Freedom of Information Act or as miscellaneous requests, depending on the nature of the data and the reason the data is being requested.

4.Key Definitions

SubjectAccess Request or SAR	A request for access to data by a living person under the Act is known as a Subject Access Request or SAR. All records that contain the personal data of the subject will be made available, subject to certain exemptions.
Freedom of InformationRequest or FOI.	A request for access to data held is dealt with under the Freedom of Information Act 2000 and is known as a Freedom of Information Request or FOI. Requests for the data of deceased people may be processed under this legislation.
Personal Data	Personal data means data which relates to a living individual who can be identified directly or indirectly from the data, particularly be reference to an identifier. Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).
Special Category Data	Certain personal data, special category data, is given special protections under the Act because misuse could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination. Special category data includes: • a person's racial or ethnic origin; • political opinions; • religious or similar beliefs; • trade union membership; • physical or mental health or condition or sexual life; • biometric or genetic data.
Data Controller	The organisation which determines the purposes and the manner in which, any personal data is processed is known as the data controller. The trust is the data controller of all personal data used and held within each part of the trust
Data Processors	Organisations or individuals who process personal data on behalf of a data controller are known as data processors. Employees of data controllers are excluded from this definition, but it could include suppliers which handle personal data on our behalf.

Data Subject	A living individual who is the subject of personal data is known as the data subject. This need not be a UK national or resident. Provided that the data controller is subject to the Act, rights with regards to personal data are available to every data subject, wherever his nationality or residence.
Third Party	An individual who is not the subject of the data but may be connected to or affected by it is known as a third party.
Relevant Professional	The practitioners who supply information held on Social Services records, and various other medical and educational records. A relevant professional will consider where disclosure is likely to cause serious physical or mental harm to the applicant or any third party.

5. Duties of the Information Commissioners Office

The Information Commissioner's Office is the UK's independent public body set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals, ruling on complaints and taking appropriate action when the law is broken.

The Information Commissioners Office is responsible for ensuring compliance with the Act and Data Protection in practice for all organisations in England, Scotland, Northern Ireland and Wales.

There are a number of tools available to the Information Commissioners Office for taking action to change the behaviour of organisations that collect, use and keep personal information. They include criminal prosecution, non-criminal enforcement and audits. The Information Commissioner also has the power to serve a monetary penalty notice on a data controller for breaches of the Act.

If organisations are found to be in breach of the Act the Information Commissioners Office may issue undertakings committing an organisation to a particular course of action in order to improve its compliance.

The Information Commissioners Office can serve enforcement notices and 'stop now' orders where there has been a breach, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law.

The Information Commissioners Office conduct consensual assessments (audits) to check organisations are complying. In cases of serious breaches, the Information Commissioners Office may issue a monetary penalty notice, requiring organisations to pay a fine of up to €20 million.

The Information Commissioners Office can prosecute those who commit criminal offences under the Act. This includes organisations and individuals.

6. Roles and Responsibilities

Adhering to the Data Protection Act 2018 is the responsibility of every member of staff acting for or on behalf of the trust. Subject Access requests fall within the data protection statutory framework and the ability to identify and appropriately handle a request for information is considered to be part of every employee's role.

Your primary responsibility is to ensure that Subject Access Requests are in the first instance directed to the Principal. The team will log the request, acknowledge it and pass the case to the trust Data Protection Officer for response. It is important that requests are processed as soon as they are received to assist in meeting the statutory deadline.

Accounting Officer	Accounting Officer holds overall responsibility for compliance with the Act.
Data Protection Officer	Data Protection Officer has responsibility for the management of Subject Access Requests; this includes dealing with complaints from the Information Commissioners Office, general compliance issues and data subject queries and concerns. Ensures that SARs are responded to in a timely manner and that only data that the data subject is entitled to access are sent out. Also responsible for completing a double check of all subject assess request's before they are securely dispatched.
Employees	All employees, including temporary staff, must understand their duty of care to ensure the confidentiality of all personal data. In addition, they must have an understanding of this policy and where to direct individuals enquiring about subject access requests.

7. How can an individual make a Subject Access Request?

A valid subject assess request must always be made in writing. Most subject assess requests are made by parents and members of staff via email or post.

It is quite common that a request for personal data can be linked with a complaint, or a Freedom of Information request.

NOTE: No matter how a request is received there is no requirement for the requester to mention either the Data Protection Act or Subject Access for it to be a valid request. In some cases, the requester may even state the wrong legislation e.g. Freedom of Information Act, but the request will still be valid.

Either way, it is the responsibility of the staff member dealing with the request to appropriately recognise a request as one for personal data, i.e. information relating to the requester, and process it accordingly. Failing to recognise a subject assess request is not an excuse for nonresponse and the trust will still fall foul of the Data Protection Act should a response not be provided in a prompt and appropriate manner.

8. Can individuals request personal information on behalf of another person?

Yes, they can. The Act allows for an individual to make a request on behalf of another person. This may be a solicitor acting on behalf of the individual, a parent making a request for their child's information, a third party making the request for someone who has limited capacity, or indeed many other reasons. However, whilst the Act allows us in certain circumstances to process a request in this way, there are a number of considerations and checks that need to

be undertaken before you process a request which is made on behalf of another person. For example, a parent is not necessarily automatically entitled to information about their children. Further information with regards to subject assess request's made on behalf of another person can be found in the Subject Access Procedure.

9.How long do we have to respond?

The trust has a maximum of a month starting from the day the request and identification (if required) is received. This is a statutory requirement which must be adhered to. In exceptional circumstances an extension can be agreed.

10. Can I charge for the request?

No - you must provide a copy of the information free of charge.

However, you can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

You may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests.

The fee must be based on the administrative cost of providing the information.

11. What do I do if I receive a request?

In practice, if someone wants to see a small part of their data (an exam result or written consent); you need to apply common sense. You should not require a formal Subject Assess Requests if the individual can prove their identity, the information is readily available there and then, and no other third party data will be unreasonably released. Such requests should be dealt with quickly, as business as usual and with little formality.

All other ("non-routine") requests for personal data which are likely to take a reasonable amount of resource must be directed to the [Data Protection Officer – to be completed by the trust when your procedure has been agreed] and be logged.

12. How do I locate the information requested?

Processing a subject access request can prove very difficult if you do not have adequate information systems in place. Well-structured file plans and standard file naming conventions within individual academies should be in place to assist in locating information easily.

Poor file management / knowledge of systems cannot be used as a reason for being unable to respond to a Subject Assess Request effectively.

Requests for information are not limited to "live" files. Subject Assess Request's cover all information held by the trust regardless of the format it is in or where it is stored, closed, archived, and in some cases even deleted information (e.g. located in outlook deleted items) should be considered as part of a request.

Unfortunately, there is no outright exemption or time threshold with regards to the amount of time it may take members of staff to locate Subject Assess Request information. Further information with regards to resource intensive or complex Subject Assess Requests can be found in the Subject Access Procedure.

13. Can I provide all information found relating to the data subject?

The simple answer is no.

The trust must consider whether it is possible to comply with the Subject Assess Requests without revealing information that relates to and identifies a third-party individual or any other exempt information.

Examples of third-party information that cannot be shared routinely without specialist consideration are:

- Safeguarding concerns which may contain information about multiple children including siblings and estranged parents
- Files containing legally privileged information
- Files containing advice from relevant professionals such as doctors, police or probation services
- Employee files containing information identifying managers or colleagues who have contributed to (or are discussed in) that file.

Special consideration should be given to sharing this type of information. More information can be found in the Subject Access Procedure.

14. What is a double check?

Before a Subject Assess Request is sent out to the data subject, the Director of Projects and Technology/Chief Finance and Operations Officer are required to carry out a double check. This is done to ensure that all third-party data has been removed appropriately and that any documents have been redacted appropriately.

Third party data sent out in error to the wrong person constitutes a data breach under the Data Protection Act 2018 and can have very serious consequences for the trust (see section 5 above).

The Director of Projects & Technology /Chief Finance and Operations Officer are responsible for completing a double check of the information to be provided to the data subject. For further guidance on the double check please refer to the Subject Access Request Procedure.

NOTE: Occasionally trusts / academies will outsource the redaction of Subject Access Requests to a third-party provider such as LBC's IG team, a solicitor or barrister. A double check of the work completed must be carried out by the Director of People, Culture and Development /Chief Finance and Operations Officer before any documents are sent out to the data subject. This is to ensure that the work is completed to the standards expected by the trust.

15. How do I respond to a Subject Access Request?

Once all of the information has been collated (duplicates and third party information has been removed or redacted and a double check has been carried out) the information will be provided either in paper copy, electronically or during a meeting with the Data Subject and sent securely.

The trust is required to provide the copies in a format requested by the data subject. For further information on how to respond securely to a Subject Access Request please refer to the Subject Access Request Procedure.

16. Complaints

The trust will provide a right of complaint to all applicants in the event they are dissatisfied with the handling of their request. If an applicant is unhappy with the service, they have received they should firstly contact the Principal.

If the applicant is dissatisfied with the content of the information, they have received they should also make a complaint in writing to the trustees. If an applicant remains dissatisfied with the outcome of their Stage 1 complaint, the trust should seek advice from your Data Protection Officer at Solent Academies Trust.

The Data Protection Officer will make an independent assessment of the case. If the applicant remains dissatisfied, they may ask the Information Commissioners Office to carry out an independent investigation.

16.1. Appealing decision to refuse disclosure of information

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a Freedom of Information request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a Freedom of Information request. Therefore, most subject access requests from parents or carers of pupils at our academies may be granted without the express permission 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.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a Freedom of Information request. Therefore, most subject access requests from parents or carers of pupils at our academies may not be granted without the express permission 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.

16.2. Complaining to the Information Commissioners Office

If an applicant is not satisfied with the outcomes of the trust's decisions, they have the right to submit a complaint to the Information Commissioners Office. The Information Commissioners Office will make an initial assessment of the case before carrying out an investigation.

The Information Commissioners Office has written guidance notes for applicants on how to complain to the Information Commissioners Office and published it on their website, www.ico.gov.uk