Subject Access Request Policy

Document Control

Version	Author	Summary of Changes	Approved By	Date Published	Date of Review
V1	RGR	New	Trust Board	Mar 2020	Mar 2021
V2	RGR	New template; change GDPR to UK-GDPR; update DPL/DPO responsibilities	Trust Board	Mar 2021	Mar 2022
V3	RGR	Annual Review	Trust Board	Mar 2022	Mar 2023
V4	RGR	Update 2. Personal Information. New: 6. Refusing to respond to a SAR; 7. Sharing data with third parties; 8. Requests in respect of crime and taxation; 9. Court orders; 10. Redaction; 11. Protection of third parties.	Trust Board	Mar 2023	Mar 2024
V5	RGR	New section 6. Exemptions	Trust Board	Mar 2024	Mar 2025

Contents

1. STATEMENT OF INTENT

This Policy is intended for anyone who submits SARs to the Trust or responds to SARs on behalf of the Trust.

Leger Education Trust collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the academies. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the trust and its academies comply with their statutory obligations.

Under the General Data Protection Regulations (UK-GDPR), individuals have the right to access their personal data. This is commonly referred to as subject access.

Individuals can make a subject access request verbally or in writing. We have created a template for individuals to use which we will share on our academies and Trust websites.

We will respond to requests within one month. We will not charge a fee to deal with requests in most circumstances. In some cases where the request is more complex, we may comply within three months, but in that case, we will write to the individual and explain why we need longer. Individuals will be made aware that we may find it harder to access this information and respond during the summer holidays.

2. PERSONAL INFORMATION

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 obtain1 such as a name, date of birth, 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:

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

3. RIGHTS OF ACCESS TO INFORMATION

Individuals are only entitled to their own personal data and not information relating to other people, unless the information is also about them or they are acting on behalf of someone.
In additional to their personal data, we will provide the information below. Our Privacy Notice provides further details about this information:

- the purposes of our processing;
- the categories of personal data concerned;
- the recipients or categories of recipient we disclose the personal data to;
- our retention period for storing the personal data or, where this is not possible, our criteria for determining how long you 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 Information Commissioner's Office (ICO) or another supervisory authority;
- information about the source of the data, where it was not obtained directly from the individual;
- the existence of automated decision-making (including profiling); and
- the safeguards we provide if you transfer personal data to a third country or international organisation.

4. CHILDREN AND SUBJECT ACCESS REQUESTS

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 subject access 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.

Infant and Junior academies:
Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our academy 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.

Secondary academies:
Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our academy 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.

5. RESPONDING TO SUBJECT ACCESS REQUESTS

Requests for information may be received verbally or in writing (including by email). Key staff such as administrators, Headteacher/Principal, pastoral staff and class teachers will be made aware of this. **We have created a template for individuals to make requests, to help make the process easier. This form is available on our academies and trust websites and can be completed electronically.** Staff receiving requests should download and use the form to record subject access requests received by any other means.
A designated person or team in each academy will be responsible for responding to requests. More than one member of staff should be aware of how to process a SAR. Requests should be notified to the Leger Education Trust Data Protection Lead (DPL) and the Data Protection Officer (DPO) – a scanned copy of the request should be emailed securely to info@legereducationtrust.com and tpinto@esafetyoffice.co.uk

When responding to requests, we:

- Will contact the individual via phone to confirm the request was made
- May ask the individual to provide 2 forms of identification. It is the individual academy's responsibility to verify the identity of the requestor before the disclosure of any information. Checks should be carried out regarding proof of relationship to the child.
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

If the initial request does not clearly identify the information required, then further enquiries will be made. All information will be reviewed prior to disclosure.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records

- Is given to a court in proceedings concerning the child

Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another academy. Before disclosing third party information, consent should normally be obtained.

Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

If there are concerns over the disclosure of information then additional advice should be sought from the Trust's DPL or DPO.

Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.
Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

Information may be provided at the academy with a member of staff on hand to help and explain matters if requested, provided at face to face handover or sent by secure email.

We will not send secure information by post.

The academy will notify the DPO when a response has been provided, and the summary letter accompanying the response.

The DPL is responsible for monitoring and reporting on all Subject Access Requests to the trustees.

6. EXEMPTIONS

In certain circumstances we may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

Crime detection and prevention:
We do not have to disclose any personal data which we are processing for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty. This is not an absolute exemption. It only applies to the extent to which the giving of subject access would be likely to prejudice any of these purposes. We are still required to provide as much of the personal data as we able to. For example, if the disclosure of the personal data could alert the individual to the fact that he or she is being investigated for an illegal activity (ie by us or by the police) then we do not have to disclose the data since the disclosure would be likely to prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders.

Protection of rights of others:
We do not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information (or that information and any other information that we reasonably believe the data subject is likely to possess or obtain), unless:

a) that other individual has consented to the disclosure of the information to the individual making the request;
   or
b) it is reasonable to disclose the information to the individual making the request without the other individual's consent, having regard to:
   i. the type of information that would be disclosed;

ii. any duty of confidentiality owed to the other individual;
iii. any steps taken by the controller with a view to seeking the consent of the other individual;
iv. whether the other individual is capable of giving consent; and
v. any express refusal of consent by the other individual.

Confidential references:
We do not have to disclose any confidential references that we have given to third parties for the purpose of actual or prospective:

a) education, training or employment of the individual;
b) appointment of the individual to any office; or
c) provision by the individual of any service.

This exemption does not apply to confidential references that we receive from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (ie the person giving the reference), which means you must consider the rules regarding disclosure of third-party data set out in paragraph 11 before disclosing the reference.

Legal professional privilege:
We do not have to disclose any personal data which are subject to legal professional privilege. There are two types of legal professional privilege:

a) 'Advice privilege' covers confidential communications between the Trust and our lawyers where the dominant purpose of the communication is the seeking or giving of legal advice;
b) 'Litigation privilege' covers any document which was created with the dominant purpose of being used in actual or anticipated litigation (e.g. legal proceedings before a court or tribunal). Once a bona fide claim to litigation privilege ends, the documents in the file which were subject to litigation privilege become available if a data subject access request is received.

Corporate finance:
We do not have to disclose any personal data which we process for the purposes of, or in connection with, a corporate finance service if:

a) disclosing the personal data would be likely to affect the price of an instrument; or
b) disclosing the personal data would have a prejudicial effect on the orderly functioning of financial markets; or
c) the efficient allocation of capital within the economy and we believe that it could affect a person's decision:
    i. whether to deal in, subscribe for or issue an instrument;
    ii. whether to act in a way likely to have an effect on a business activity, eg on the industrial strategy of a person, the capital structure of an undertaking or the legal or beneficial ownership of a business or asset.

Management forecasting:
We do not have to disclose any personal data which we process for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity.
Examples of management forecasting and planning activities include student performance, staff relocations, redundancies, succession planning, promotions and demotions. This exemption must be considered on a case by-case basis and must only be applied to the extent to which disclosing the personal data would be likely to prejudice the conduct of that business or activity.

Negotiations:
We do not have to disclose any personal data consisting of records of our intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations. For example, if the HR department is negotiating with an employee in order to agree the terms of a redundancy package and the employee makes a data subject access request, the HR department can legitimately withhold giving access to information which would prejudice those redundancy negotiations. The HR department must,

however, disclose all other personal data relating to the individual unless those other personal data are also exempt from disclosure.

7. REFUSING TO RESPOND TO A SAR

Per GDPR (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. 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.

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.

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.

In either case a school needs to justify the decision and inform the requestor about the decision. 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.

8. SHARING PERSONAL DATA WITH THIRD PARTIES

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

If a request is made by a third party seeking the personal data of the data subject (e.g. a solicitor acting on behalf of a client), the school needs to be satisfied that the third party making the request is entitled to act on behalf of the individual. This might be a written authority to make the request or a more general power of attorney. Academies should request the third party to confirm what identity checks have been carried out prior to releasing documents. It is the third party's responsibility to provide evidence of this entitlement. The school should not contact the data subject directly for such evidence.

If the school has any concerns as to providing the personal data of the data subject to the third party, then the information requested should be provided directly to the data subject. It is a matter for the data subject to decide whether to share this information with any third party.

Consent to disclose a data subject's personal data to a third party is only valid if such consent is freely given. If the 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.

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.

Where a school has personal data relating to both the request and data subject then the 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.

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, providing the student has given consent to disclosure. The law assumes that the student will see the disclosure.

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
- 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 cannot access this information
- any views the pupil has on whether their parents or carers should have access to information about them

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

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

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

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.

Schools are not legally obliged to provide the information.

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

10. COURT ORDERS

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

11. REDACTION OF INFORMATION

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.

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 will also refer to the ICO's guidance "How to disclose information safely - removing personal data from information requests and datasets".

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.

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.

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.

A second person authorised by the Headteacher is required to check that all necessary redactions have been made before disclosure in cases where the DPO has not undertaken the redaction.

All draft SAR responses and redacted documentation must be sent securely to the Trust's DPL for review prior to their issue by a school to a requestor, unless the DPL has undertaken the redaction and determined whether any exemptions are to be applied.

12. PROTECTION OF THIRD PARTIES – EXEMPTIONS TO THE RIGHT OF SUBJECT ACCESS

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 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
- 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 Trust's business or activities
- Complaints
- Legal professional privilege
- Exam Scripts and Marks – 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 - safeguarding concerns may contain information about multiple children including siblings and estranged parents; files containing advice from doctors, police or probation services.

Where personal data is not to be provided due to application of an exemption, schools should ensure internal documentation is in place regarding its reasoning for withholding this data. The personal data withheld and exemption applied should also be recorded in the Trust's SAR Log.

13. COMPLAINTS

We take any complaints about our collection and use of personal information very seriously.
If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.
To make a complaint, please contact our data protection officer

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

14. CONTACT US

If you have any questions, concerns or would like more information about anything mentioned in this policy, please contact our:

Data Protection Lead:
Rebecca Grange
Executive Director of Operations
Leger Education Trust
Ryecroft Road
Norton
Doncaster
DN6 9AS
Tel: 01302 700002
info@legereducationtrust.com

Data Protection Officer:
Tim Pinto
E-Safety Office
Mobile: 07595302684
VOIP: 01977 232167
Email**:** tpinto@esafetyoffice.co.uk
Web: www.esafetyoffice.co.uk

APPENDIX 1 - SUBJECT ACCESS REQUEST FORM

Under the General Data Protection Regulations, individuals have the right to request access to the information we hold about them.
We've created this template for you to help make the process easier.
We will provide this information free of charge and within one month. In some cases where the request is more complex, we may comply within three months, but in that case, we will write to you and explain why we need longer. Please be aware that we may find it harder to access this information and respond during the summer holidays.
We will telephone you to confirm the request is genuine and we will also need to check your identity, usually by asking for two forms of identification.

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 SEND records*