Academies Trust

8th Floor, Angel Square,
Manchester, M60 0AG

Subject Access Request Policy

Approved by Trust Board on 13 July 2018
Applicable from 1 September 2018

1.0 Purpose

The Co-op Academies Trust (the Trust) and its academies are required to follow the General Data Protection Regulation (GDPR) in the way that they collect and use personal data. Chapter 3 of the GDPR sets out the rights of individuals with regards to their personal data.

This policy sets out the approach that will be taken by the Trust's central team and its academies to deal with requests by individuals to exercise one or more of the rights they have towards their personal data.

This policy applies to:

- All employees of the Trust whether based in an academy or in the Trust's central team
- Trust Board members and governors

2.0 Introduction

The GDPR describes the responsibilities that organisations have when dealing with personal data. Personal data is defined as any information relating to an identified or identifiable natural person. The person is known as a 'data subject'.

The GDPR provides data subjects with rights in respect of their personal data. Data subjects have the;

- Right of access by the data subject
- Right to rectifications
- Right to erasure ('right to be forgotten')
- Right to restriction of processing
- Right to data portability
- Right to object
- Right not to be subject to automated individual decision making, including profiling

The nature of the personal data and the reason for its use determine which of these rights are applicable. Annex 1 sets out the types of data that the various rights apply to.

As educating, supporting and developing young people is at the heart of the Trust's and its academies work, there are certain circumstances where a parent or another legal representative may exercise these rights on behalf of the young person. Annex 2 sets out the factors that determine whether the young person or their parent or legal representative is empowered to exercise these rights.

3.0 Related Policies

This policy is closely linked with other Trust and Academy policies which should referenced when appropriate, including:

- Safeguarding and Child Protection
- Data Protection
- Staff Code of Conduct, including Electronic Communications
- Any other relevant guidance documents

4.0 Responsibilities

Trust's academies and their governing bodies will:

- Put in place a clear procedure for dealing with the requests of data subjects or their legal representatives to exercise their rights in respect of their personal data. This procedure should take account of the requirements laid down in Annex 3.
- Follow any additional guidance from the Trust or the Information Commissioner's Office (ICO) produced subsequently to this policy
- Inform the Trust's Data Protection Officer of requests that are made
- Record the details of requests made in the system provided by Trust for this purpose
- Record the results of the request and communications with the data subject or their legal representative
- Ensure that requests are dealt with in line with the statutory limit for the type of request and notify the Trust's Data Protection Officer as soon as possible if these limits can't be met
- Consult with the Trust's Data Protection Officer if there are concerns about the nature of the request or of its' validity

The Trust will:

- Provide guidance and support to any academy dealing with a data subject request
- Provide a route of communication to the ICO in the event of difficulties in delivering the required request

5.0 Review

The Trust's policy on Data Subject requests will be reviewed annually, or when the ICO issues revised guidance on this topic.

Annex 1

Application of data subject rights

The rights applicable to a certain piece of personal data depend upon the lawful basis of the processing. It should be noted that there may be some categories of personal data that rights will be applicable to a specific purpose of processing, where the same rights will not exist for a different purpose of processing.

1. Right of access by the data subject

This right is available to all data subjects. It should be noted that access to the data is subject to a range of exemptions which are discussed further in Annex 3

2. Right to rectification

This right is available to all data subjects. It relates to inaccurate data and care must be taken when the data is based on professional opinion. It is possible for the data subject to have incomplete data completed by providing a supplementary statement.

3. Right to erasure

This right does not apply to personal data that is being processed on the basis of

- Exercising the right of freedom of expression and information
- Compliance with a legal obligation to which the controller is subject
- The performance of a public task
- Archiving for scientific or historical purposes
- The establishment, exercise or defence of legal claims

4. Right to restriction of processing

This right applies to data processed under any lawful basis. There are restrictions to the circumstances that must apply to enable the restriction to be put in place; they are detailed in Article 18 of the General Data Protection Regulation.

5. Right to data portability

This right only applies to data being processed on the basis of consent or for the purposes of a contract. Furthermore, it relates only to data provided by the data subject that is processed by automated means (i.e. By computerised systems). This includes two classes of personal data

- Data knowingly provided by the data subject
- Observed data provided by the use of the data subject of a service or device

Within the context of education this produces a significant restriction on the data that would be accessible.

6. Right to object

This right only applies to data processed on the basis of a public task or under legitimate interest. This includes the majority of data that schools process in relation to students, parents and visitors but not members of staff.

7. Right not to be subject to individual decision making based on automated processing, including profiling

This right applies to personal data processed for legal compliance, in the vital interests of the data subject, data processed for a task in the public task and for legitimate interests.

Although it doesn't apply to data processed under consent or contract, data controllers are required to offer data subjects the opportunity to request human intervention to put their case if they consider the decision is wrong.

Similarly, if the decision making is authorised by the member state then providing there are suitable safeguards to the data subject's rights and freedoms then the right is not applicable. This means that it's likely that any decision making made by statutory requirement would be exempt from the right.

Subject Access Requests about children

The ICO guidance about Subject access requests form June 2017 sets out the following:

"Even if a child is too young to understand the implications of subject access rights, data about them is still their personal data and does not belong to anyone else, such as a parent or guardian. So it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.

Before responding to a SAR for information held about a child, you should consider whether the child is mature enough to understand their rights. If you are confident that the child can understand their rights, then you should respond to the child rather than the parent.

What matters is that the child is able to understand (in broad terms) what it means to make a SAR and how to interpret the information they receive as a result of doing so. When considering borderline cases, you should take into account, among other things:

- *where possible, the child's level of maturity and their ability to make decisions like this;*
- *the nature of the personal data;*
- *any court orders relating to parental access or responsibility that may apply;*
- *any duty of confidence owed to the child or young person;*
- *any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;*
- *any detriment to the child or young person if individuals with parental responsibility cannot access this information;*
- *any views the child or young person has on whether their parents should have access to information about them.*

In Scotland, the law presumes that a child, aged 12 years or more, has the capacity to make a SAR.

The presumption does not apply in England and Wales or in Northern Ireland, but it does indicate an approach that will be reasonable in many cases. It does not follow that, just because a child has capacity to make a SAR, they also have capacity to consent to sharing their personal data with others as they may still not fully understand the implications of doing so."

The Information Commissioner's Office is still in the process of developing guidance about the use of consent in relation to personal data held about children. These rules may change once that guidance has been produced.

In the context of subject access requests, in England, a judgement must be made about the capability of a child aged 12 or over. The factors above are there to help guide the decision making process.

The guidance assumes that the request goes forward irrespective of the age of the child with the data being delivered to the child. The child then has the option of delivering the

data to the parent or not. This approach can be seen to be inconsistent with the fact that it is an offence to force a data subject to make a subject access request.

Furthermore, by asking a child if they consent to an access request it may obviate the requirement to retrieve and construct significant amounts of information

Annex 3

Requirements of the procedure for managing data subject request

1. Subject Access Request Team (SAR team)

In order to respond to requests consistently and efficiently, the Trust and its academies require the permanent formation of a Subject Access Request Team which comes together on receipt of a request.

The Subject Access Request Team for the Trust's central team, will respond to requests relating to data processed by its central teams. The team will deal with all request types, not just subject access requests.

This Subject Access Team will be managed by the Trust's Data Protection Officer (or cover DPO) and will additionally comprise representatives of each area of the central team's functions. The Trust's Subject Access Team (for its central teams) therefore comprises:

- The Data Protection Officer (and Governance Manager)
- The Finance Manager
- The Communications and Marketing Manager
- The HR Officer
- The Governance and Administration Officer

Each academy' will have its own subject access team which will respond to all request types relating to data processed by their academy. The membership of these teams will reflect the membership of the Subject Access Team for the Trust's central team. Additionally, academies will appoint one or more member of staff to fulfill the role of primary point of contact (PPOC) for all requests. Academies' teams will be managed by the GDPR Ambassador. The Trust's DPO (or cover DPO) should be notified as soon as possible of any serious or complex requests.

2. Procedure overview

The procedure for managing all data subject requests is mostly common to all types of response, the specific delivery differs and this is set out in the section on those specific procedure steps. The procedure is:

i. Receive a request
ii. Collect details of the request
iii. Verify the identity of the requestor
iv. Validate the request
v. Collate information / undertake action
vi. Deliver information / update requestor

3. Receive a request

The request may be initiated across many channels. It may be written in an email, a letter or across an official school social media account. It may start as a voice message or be addressed directly to a member of staff.

Members of staff should review their email regularly (including spam folders) to ensure they have not received a request. During periods of leave, an out of office message must be in place with clear instructions of an available contact.

Voicemail should also be checked regularly and for the main school system an option should be considered to direct data subjects to a channel to deliver requests outside of term time.

Administrators of the social media channels of an Academy are responsible for monitoring incoming posts or messages to identify potential data subject requests.

All communications that appear to be data subject requests should be referred initially to the PPOC for the Academy.

4. Collect details of the request

All academies, and the central team have access to the Sentry Online system. This can register a data subject request and it is the location where the definitive record should be kept.

In the first instance it is suggested that a form be used for data subjects to capture their requests. This may be completed directly by the data subject or with the assistance of someone from the SAR team.

A signature from the data subject once they are happy with the request will help to limit misunderstanding although this can't be demanded before proceeding. A scanned copy of the form should be attached to the request in Sentry Online.

The team may ask the data subject if they wish to restrict access to specific records but may not demand any such limitation.

Where the request is not for access, it is essential that the details of the request are clear. For rectification requests the data subject will need to include evidence to support the changes that they wish to make to the records. Copies of the evidence provided should be scanned and attached to the request record.

5. Verify the requestor

In order to avoid the potential for data subject requests becoming a source of personal data breaches, it is essential to verify the identity of the requestor. The level of verification depends on the person making the request.

Where the requestor is a member of staff or a student then sufficient informational already exists to verify the individual. This normally will come from the photograph used for identification purposes (perhaps stored on SIMS) and day to day knowledge of the person.

Whenever possible the data subject should be asked to present themselves in person for verification. The PPOC is likely to be responsible for conducting ID verification.

Where the requestor is not known then standard ID verification is used. A piece of photo ID and a utility bill or equivalent can be used. Although a note can be made of the documents presented (eg Driving Licence and Water Bill) no personal details from these documents needs to be stored (eg copies)

In the case of a requestor unable to attend in person, advice should be sought from the Trust's Data Protection Officer who can help facilitate remote verification.

Where the requestor is a legal representative, evidence should be required to show that they do possess rights in relation to the individual about whom data is sought. Copies of this documentation should be made and attached to the request file. For parents or family who are not listed as contact points for a child, then similar documentation should be requested to show that they are entitled to obtain information.

6. Validate the request

A decision needs to be made in relation to the request made about whether the request can be met. There are a number of reasons why a request may not be met. For example:

- The requested right does not apply to the personal data
- Requested data may be exempted from release
- If the requestor is not the data subject, the data subject may not consent to the release of the data
- Insufficient evidence has been provided for a rectification request

The decision on whether data can be released or whether a request can be completed should be taken by the GDPR Ambassador. Reference should be made to the Subject Access Request code of practice published by the ICO around exemptions.

If there is any doubt about the validity of the request then advice must be sought from the Trust's Data Protection Officer before proceeding.

7. Collate information / undertake request

For subject access requests the academy data mapping holds details of where information is kept. Depending on the nature of the request, it may be necessary to request that individuals search email to find personal data that they may be holding and forward this to the SAR team.

Depending on the IT facilities available then data may need to be copied into an application to enable a pdf copy to be produced. Various tools can be bought to perform the same function. Adobe Acrobat (£181 per year subscription) allows multiple files to be combined to produce a single pdf and allows a watermark to be applied.

The copy to be provided to the data subject should be marked 'Data Subject Copy' another copy marked 'Data Controller Copy' should be stored along with the details of the request.

Other actions, like rectification or providing a portable copy of relevant personal data should be undertaken if required. For these more unusual requests, support should be sought from the Trust's Data Protection Officer.

8. Deliver the results / inform requestor

Where the results of a request have been gathered then it needs to be provided to the requestor. Although the initial request is free of charge, it is permissible to charge for further copies of the data. If you're unsure whether a charge can be levied, seek advice from the Trust's Data Protection Officer.

It is assumed that unless specifically requested, the results of a request will be communicated electronically. This can be the same pdf produced to give access. Unless a verified email address is in use then email is unlikely to be a secure route for delivery of the data. Some form of download system would be preferable that required a positive sign in by the user.

If it has not been possible to validate the requestor then the requestor should be informed. Care should be taken that informing the requestor does not reveal the existence of information that is exempted from release.

For other requests where a definitive result is not produced, you should inform the requestor that the request has been successfully completed.

9. Timing

Standard subject access requests have a return period of one calendar month as does a request for portability. Other requests should be completed without undue delay once verification and validation are complete.

If an access request can’t be validated, you should inform the requestor without undue delay once the determination has been made.