East Midlands Academy Trust

Data Protection SAR Policy 2021/2023

'Every child deserves to be the best they can be'

Scope: East Midlands Academy Trust & Academies within the Trust	
Version: V1	**Filename:** EMAT Data Protection – Subject Access Request Policy
Approval: April 2021 *Approved by the Trust Board*	**Next Review: April 2023** *This Policy will be reviewed by the Trust Board (A&R committee) every two years*
Owner: Head of Shared Services	**Union Status:** Not Applicable

Policy type:	
Non-Statutory	Replaces Academy's current policy

EMAT Data Protection – Subject Access Request Policy

1 Purpose

The East Midlands Academy Trust (the Trust) is required to follow the Data Protection Act (2018) (the Act) in the way that it collects and uses personal data. The Act references and implements the General Data Protection Regulation (UK GDPR) with some specific amendments.

Chapter 3 of the UK GDPR sets out the rights of data subjects with respect to their personal data. Although the most common right is Subject Access, there are many others. As a group these referred to as 'data subject requests'. The regulations set out the steps that data controllers need to put in place to allow data subjects to exercise these rights.

This policy sets out the approach that the Trust will take to deal with data subject requests. This policy applies to all employees of the Trust.

Our Data Protection Officer is:

Name of DPO:	GDPR Sentry Limited
email address:	support@gdprsentry.com
Contact number:	0113 804 2035
Contact address:	Unit 434 Birch Park, Thorp Arch Estate, Wetherby, West Yorkshire, LS23 7FG

2 Introduction

The UK 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 UK GDPR provides data subjects with rights in respect of their personal data. Not all rights apply in respect of all personal data. Data subjects have the following rights:

- Right of access by the data subject
- Right of rectification
- Right of erasure ('right to be forgotten')
- Right of restriction of processing
- Right of data portability
- Right to object to processing
- 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. Guidance about whether a particular right is applicable should be sought from the Data Protection Officer.

When a data subject seeks to exercise one of these rights it is called a data subject request. The most common data subject request is a subject access request (SAR)

As the Trust deals with young people, there are certain circumstances where a parent or another legal representative may exercise these rights on behalf of the young person. Any situations where there is a question over rights to access personal data or the exercising of these other rights must be referred to the Data Protection Officer.

3 Related policies

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

- Data Protection Policy
- Child protection
- Safeguarding
- Any other relevant guidance documents

4 Responsibilities

The Trust will:

4..1 Put in place a clear procedure for dealing with data subject requests. This procedure should take account of the requirements laid down in Annex 1.

4..2 Follow any additional guidance from the Information Commissioner's Office (ICO) produced subsequently to this policy

4..3 Inform the Data Protection Officer of all data subject requests

4..4 Record the details of data subject requests and make those records available to the Data Protection Officer

4..5 Ensure that data subject requests are dealt with in line with the statutory time limits and notify the Data Protection Officer as soon as possible if these limits can't be met

4..6 Ensure that proper account is taken of the risk of disclosing information about a third party in responding to a data subject request and the risk of failing to maintain the availability and integrity of the personal data it processes.

4..7 Take advice from the Data Protection Officer with regards to the management of data subject requests

The Data Protection Officer will:

4..1 Provide guidance and support to the Trust in dealing with a data subject requests.

4..2 Provide a route of communication to the Information Commissioner's Office in the event of issues with the content or timing of responses to a data subject request.

5 Implementation of policy

This Policy shall be deemed effective on 16/03/2021. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

6 Review

This policy on data subject requests will be reviewed bi-annually, or when the Information Commissioner's Office (ICO) issues revised guidance on this topic.

Annex 1: Procedure for managing data subject requests

1. Data subject request response team

Requests from data subjects can create significant work, especially in the case of subject access requests. Other types of requests, such as objections to processing have the potential to disrupt the normal operation of the Trust.

Failing to meet the requirements of a data subject request can result in enforcement action by Information Commissioner's Office and it is arguable that for the Trust the reputational damage is a greater risk than any potential fines.

This being the case, the delivery of data subject's requests needs to be managed by staff who are able to collect appropriate data or take the actions requested by the data subject without administrative delay.

The Trust has a Data Protection Team. This team comprises a permanent core team, supplemented by other members depending on the nature of the request being managed.

This Data Protection Team will be managed by the Director of Operations or and will also include

The Data Protection Officer

And include staff from:

- Shared Service
- A member of senior leadership from each academy in the trust
- Finance
- Governance
- HR
- Include others as appropriate

This teams need to reflect representation of the major functions within The Trust (Senior Leadership, Teaching and Learning, Administration and IT).

2. Procedure overview

The procedure for managing data subject requests needs to be implemented in detail by the Data Protection Team across the Trust. These procedures need to take account of the following stages and requirements. The actions described in this section are by no mean exhaustive. The Data Protection Team may establish further detailed procedures and work instructions. Where this happens, they will be referred to in the main body of this policy.

I. Receiving a data subject request
II. Clarifying a request
III. Verifying the identity of the requestor
IV. Validating the request
V. Fulfilling the request
VI. Communications with the requestor

3. Receiving a data subject request

Unlike the 1998 Data Protection Act, there are no restrictions on how a person can register a request in respect of personal data belonging to them or a third party. Any member of staff of the Trust could be approached to commence a request.

It is, therefore, essential that all staff are made aware that they may receive the initiation of a request. This can come through any communications channel that the Trust provides, and this does include a verbal request made to member of staff.

For the avoidance of doubt these channels include any social media accounts managed by the Trust, web-based enquiry forms and any voicemail systems in operation. Where email messages are distributed from accounts that are unmonitored, they must clearly state that no action will be taken on any messages sent to that address.

To clarify further, the Trust is not permitted to require data subject to complete a specific request form to initiate a subject access request.

The Trust can choose to make a specific communications route available for making data protection requests or raising questions and complaints.

The Trust encourages the use of [preferred email address] for making data subject requests, although it recognises the right of individuals to make requests through any available route.

The Trust may choose to devote an area of the it's website to register requests. The Trust cannot refuse to deal with a request if it does not use the preferred route, nor require the data subject to resubmit the request.

The complexity and potential issues of responding to a data subject request means that it is not appropriate for staff outside of the Data Protection Team to respond. The primary responsibility of staff is to ensure that any request is passed on to the Data Protection Team. In the case of an enquiry being made in person, arrangements should be made for the person to speak with a member of the data protection team, whether face to face or remotely

The Trust will set up appropriate routes for staff to notify the Data Protection Team.

This will include both telephone and email routes and provide details for contact outside of normal working hours or outside of term time. To notify a data subject request in person please speak, in the first instance to Data protection administrator:

- **Name of Person:** Daryl Unitt
- **email address:** daryl.unitt@emat.uk
- **Contact number**: 07342 712201
- **Contact address:** East Midlands Academy Trust,
  Pyramus House, Roman Way, Grange Park,
  Northampton, NN4 5EA

It is important to recognise that the delivery time for a response to a subject access request is a maximum of one calendar month. This delivery window does not take account of the academic calendar. For example, a request can be received outside of term time and it is still expected to be delivered in the standard timescale.

The Trust has put measures in place to ensure that these communications routes are monitored outside of term time.

All incoming requests should be logged in a way that is available for the DPO to review.

4. Clarify the request

It is possible that this stage is not necessary if the data subject has been very specific in their request. In most cases there is additional information required to ensure that the Trust has an accurate description of the action required.

This is most commonly seen with subject access requests where the lack of specificity by the data subject results in the entire personal data set relating to the individual being required. This can include records from IT Security equipment and entry management systems.

Especially where the potential dataset is very large, then a member of the data protection team may ask the requestor if they have any information that would enable the scope of the request to be reduced.

In the event that the relationship between the Trust and the data subject is very poor, this communication may be passed over to the data protection officer, whose role includes acting as an advocate for the data subject.

Although the Trust may ask the data subject to provide additional information to narrow the scope of the request, the data subject is under no obligation to do so. This may affect decisions about the validity of the request at a later stage in the procedure.

5. Verification of identity

If the Trust should respond to a data subject request, assuming that the person making the request is who they claim to be, and that results in some form of unauthorised disclosure or action, a breach has occurred that the Information Commissioner's would view as having been avoidable.

The UK GDPR (Recital 64) requires data controller to use all reasonable efforts to verify the identity of the person making the request. This is particularly the case when the initial request is not received in person. The means of identification should also account for the existing relationship between the Trust and the data subject. In the case of a current student or member of staff then it is easy to establish their identity in person and through the use of Trust provided communications otherwise.

For other data subjects the Trust will go through a standard form of identity verification using photo identification and proof of address. In the case that the data subject can not attend in person to present the documents, copies can be sent to the Trust and a videoconference can be used to check the person against the documents provided.

If this method cannot be used, the data protection officer should be consulted to look at alternatives.

If suitable verification is not possible then the request will not progress further.

Given the cohort at the Trust, special attention must be paid to any requests coming from parents of students for information about the student. Decisions will need to be taken about student's capacity to understand the consequences of the request for personal data, or some other data subject request. Where a data subjects is adjudged to have capacity it is expected that the request should be referred to the data subject directly.

Alternatively, the data subject can provide permission for the third party to complete the request. The same level of checking should be applied to the permission provided by the requestor and without suitable evidence the request cannot move forward.

For the avoidance of doubt, third parties such as Solicitors, Local Authorities and the Police Service cannot make a subject access request on behalf of a third party without appropriate consent. As an example, a letter from a solicitor saying that they are acting on behalf of an individual would not be sufficient without additional evidence.

There is no requirement to retain the evidence of identity gathered at this stage of the process, but the work done to establish identity should be recorded in the log of the request.

6. Validate the request

This stage is quite short. The requestor has been verified as an individual who is authorised to make a request. However, it is not the case that all data subject requests are available for all personal data. The key driver of the difference in rights available to a data subject is the legal basis of processing.

If there is uncertainty about the applicability of any particular right to particular items of personal data, the DPO should be consulted. However, it is the case that the right of access and the right to rectification apply irrespective of the legal basis of processing.

The decision about validity and any associated communications should recorded in the log of the request.

7. Fulfilling the request

Depending upon the nature of the data subject request this stage may be very short or extensive. Where the request is, for example the correction of an inaccurate item of personal data, this request should be met as soon as possible and requires limited effort. For the remainder of this section we will discuss the fulfilment of a subject access request which represents the greatest potential work.

The request will specify the data that is required to be collected. Details of locating that data can be drawn from the Record of Processing Activities. Data may be collected on paper and electronically. Electronic collection usually means getting an extract from a system containing the relevant information.

There are complex rules about the data that can be released and once the basic data has been collected these rules need to be considered. It is not possible to detail out all the potential exemptions to release and the exemptions to the exemptions.

In addition, any references to third parties should be redacted from the collected data before it can be released. Accidentally releasing information about third parties by failing to redact the response to a subject access request is generally considered a serious breach.

In some cases, where the task of redaction is unfeasible (most often with CCTV footage) a decision may be made that the information cannot be released even though it represents personal data of that data subject.

In some cases, other policies will override the data protection policy in respect of releasing information. This is especially the case with safeguarding information.

Where data is redacted or withheld, a record should be added to the log of the request.

8. Communications with the requester

Once the request has been fulfilled, for example a rectification has been done, or the response to a subject access request has been assembled, there is a requirement to communicate the response to the requestor.

In addition to the confirmation of the completion of the request the data subject or requestor should also be sent a copy of the privacy notice that is appropriate to them. This will meet the requirements to provide information about the way that personal data is processed.

Where the request was for subject access the results must be delivered to the requestor. For electronic responses a secure download, addressed to a validated email account is the preferred method.

On no account should the results be sent by email, a public sharing site, such as Dropbox, or on a removeable drive.

Where the response is provided on paper, then ideally the individual should come in person to pick up the response and sign a receipt to confirm they have received the information. If this is not possible then the results should be sent by recorded delivery to a verified postal address, or if appropriate the results can be hand delivered, double enveloped.

In the case that the request cannot be met in the stipulated calendar month, a communication must be sent to the data subject setting out the reasons for the delay and the expected timescale for the completion of the request, this communication should be sent by the data protection officer.