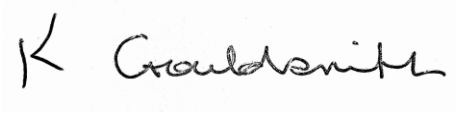
ACE Schools Multi Academy Trust

Subject Access Request Policy

Issue	Date	Author/Reviewer Job Role	Comments	Signed by DPO
	12/3/19	*Kristy Gouldsmith*		

Contents

1 Introduction

1.1 ACEMAT holds personal data (or information) about candidates, employees, trainees, pupils, parents, governors, trustees, suppliers, business contacts and other individuals for a variety of business purposes.

1.2 Under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA), individuals (known as 'data subjects') have a general right to request access to personal information or data that we hold or process about them, subject to certain exceptions. These requests are known as 'subject access requests'.

1.3 The Data Protection Officer (DPO) is responsible for ensuring:

1.3.1 that all subject access requests are dealt with in accordance with the GDPR and the DPA; and

1.3.2 that all staff have an understanding of the GDPR and the DPA in relation to subject access requests and their personal responsibilities in complying with the relevant aspects of the GDPR and the DPA.

1.4 This policy provides guidance for staff members on how subject access requests should be handled and is intended for internal use. It is not a privacy policy or statement and is not to be made routinely available to third parties.

1.5 This policy is aimed primarily at those members of staff who are authorised to handle subject access requests. For other staff members, it provides guidance on:

1.5.1 what to do if you receive a subject access request (see paragraph 2 below); and

1.5.2 how to decide whether a request for information is a subject access request (see paragraph 3 below).

1.5 Failure to comply with the GDPR puts both staff and ACEMAT at risk, and so ACEMAT takes compliance with this policy very seriously. Failure to comply with any requirement of the policy may lead to disciplinary action, which may result in dismissal.

1.6 If you have any questions regarding this policy, please contact the DPO.

2 Receiving a subject access request (non-authorised staff)

2.1 If you receive a subject access request and you are not authorised to handle it, you must immediately take the steps set out in paragraphs 2.3 (request received by email) or 2.4 (request received by letter). There are limited timescales within which we must

respond to a request and any delay could result in our failing to meet those timescales, which could lead to enforcement action by the Information Commissioner and/or legal action by the affected individual.

2.2 For information on what amounts to a subject access request, see paragraph 3 below. If you are in any way unsure as to whether a request for information is a subject access request, please contact the DPO.

2.3 If you receive a subject access request by e-mail, you must immediately forward the request to the DPO.

2.4 If you receive a subject access request by letter you must:

2.4.1 scan the letter; and

2.4.2 send a scanned copy of the letter to DPO.

2.5 You must not take any other action in relation to the data access request unless the DPO has authorised you to do so.

3 What is a subject access request?

3.1 A subject access request is a request from an individual to be given access to personal data which we process about him or her. For example, a letter which states 'please provide me with a copy of all the information that you have about me' will be a subject access request even though it does not expressly refer to personal data or to the GDPR.

3.2 All subject access requests should be immediately directed to the DPO in accordance with paragraph 2 above.

4 Requirements for a valid request

4.1 For a subject access request to be valid, the following requirements must be satisfied:

4.1.1 the request must be in writing. If an individual makes a subject access request by telephone or in person, he or she should be asked to put the request in writing, preferably using the Subject Access Request Form;

4.1.2 the requests are generally free except if they excessive, vexatious or repetitive.

4.1.3 we must be able to identify the individual making the subject access request and then verify that identity. Typically, we will request a copy of the individual's driving licence or passport to enable us to establish his or her identity and

signature (which should be compared to the signature on the subject access request and any signature we already hold for the individual). We also ask for a recent utility bill (or equivalent) to verify the individual's identity and address. We must be able to identify the information being requested. For example, if a subject access request is made by an individual who is both an employee and a customer, we can ask the individual to specify whether he or she is seeking access to human resources information, customer records or both. If the request relates to CCTV images, it may be necessary to ask the individual to supply a photograph of him or herself, or provide a description of the clothing the individual was wearing at the time his or her image is believed to have been recorded on CCTV. We should also ask for details of the date, time and location to help narrow the search further (if such information is available).

4.2 If the individual makes a request that does not satisfy the above requirements you should write to him or her setting out in what respect the requirements are not satisfied.

4.3 If the above requirements are not met, we need not comply with the subject access request immediately. However, we must notify the individual promptly (as applicable) that the fee (if required) is missing or that additional information is required in order to fulfil the request.

5 Time limit for responding to a request

5.1 Once a valid subject access request is received, we have 30 days in which to respond, unless it is a very large request, then we will have an additional 60 days. During the first 30 days, we need to inform the data subject that we need additional time.

6 Information to be provided in response to a request

6.1 The individual is entitled to receive a description of the following:

6.1.1 the personal data we process about him or her;

6.1.2 the purposes for which we process the data;

6.1.3 the recipients to whom we may disclose the data;

6.1.4 the information constituting his or her personal data;

6.1.5 any information available regarding the source of the data;

6.1.6 the logic behind any automated decision we have taken about him or her (see paragraph 6.3 below).

6.2 The information referred to in paragraph 6.1 must be provided in an intelligible, or permanent, form (eg a photocopy or print-out), and any technical terms, abbreviations or codes must be explained to the individual.

6.3 Information about the logic behind automated decisions: If the subject access request specifically asks for information about the logic behind any automated decision that we have taken in relation to important matters relating to the individual (eg performance at work, creditworthiness, reliability or conduct), we must provide a description of the logic involved in that automated decision, subject to the following conditions:

6.3.1 the automated decision must have constituted the sole basis for the decision. For example, an application for credit which is conducted without any human intervention, other than to complete the application form, could be a decision which is taken solely by automatic means. However, if there is any element of human discretion as to whether or not to grant the credit, the decision would cease to be wholly automated and the individual would not be entitled to a description of the logic;

6.3.2 in providing a description of the logic we are not required to reveal any information which constitutes a trade secret (eg the algorithm behind a credit scoring system).

7 How to locate information

7.1 The personal data we need to provide in response to a subject access request may be located in several of our electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

7.2 Depending on the type of information requested, you may need to search all or some of the following:

7.2.1 electronic systems, eg databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data, CCTV;

7.2.2 manual filing;

7.2.3 data systems held externally by our data processors;

7.2.4 occupational health records;

7.3 You should search these systems using the individual's name, employee number, customer account number or other personal identifier as a search determinant.

8 Information to be supplied in response to a request

8.1 Once you have carried out the search and gathered the results, the DPO will select the information to be supplied in response to the subject access request. The individual is only entitled to receive information which constitutes his or her personal data.

8.2 The type of information that will be classified as personal data is any information which identifies the individual, either directly.

8.3 Information about companies or other legal entities is not personal data. However, information about sole traders or partnerships will be, as the individuals within them are individuals. Personal data relating to deceased persons are not covered.

8.4 The right of access is subject to a number of conditions and exemptions, particularly where the personal data reveal information about another individual—these are covered in paragraphs 10 and 13 below.

8.5 We are required to provide this information and can choose to meet this obligation by providing to the individual a copy of pre-existing, original documents containing the personal data (redacted as necessary to remove third-party personal data and give effect to any exemptions available). Where the information includes CCTV images, we should provide the images in a way that enables them to be seen clearly (eg on disk unless the individual requests them in hard copy form) and redacted as necessary.

9 Disclosing personal data relating to third parties

9.1 If the requester's personal data includes information that identifies a third-party individual (eg as a source or recipient of the requester's personal data), you should consider the following:

9.1.1 Does the information relate to and identify the third party? In deciding this point, you should take into account:

9.1.1.1 the information you are disclosing; and

9.1.1.2 any information you reasonably believe the requester may have, or may get hold of, that would identify the third party.

9.2 If so, is it possible to comply with the request without revealing the third party's information, eg by redacting (blanking out) names or editing documents?

9.3 If it is impossible to separate the third party's information from that requested and still comply with the request, then you should consider whether the third party has consented to the disclosure of his or her information. It is good practice to ask relevant

third parties for consent to the disclosure of their personal data in response to a subject access request. However, it may not always be appropriate to ask for consent, eg if to do so would inevitably involve disclosing personal data about the requester to the third party.

9.4 If the third party has not given consent, is it otherwise reasonable in all the circumstances to disclose without the third party's consent? You should take into account the following (non-exhaustive) list of factors:

9.4.1 any duty of confidentiality that we owe to the third party;

9.4.2 any steps we have taken to obtain the consent of the third party;

9.4.3 whether the third party is capable of giving consent; and

9.4.4 any express refusal of consent by the third party.

9.5 The following additional factors should also be considered:

9.5.1 whether the third party is a recipient or one of a class of recipients who might act on the data to the requester's disadvantage;

9.5.2 whether the third party is the source of the information;

9.5.3 whether the information is generally known by the requester; and

9.5.4 the importance of the information to the requester.

9.6 Ultimately, whether or not it is reasonable to disclose the third party's information will depend upon all the circumstances and each request must be considered on a case-by-case basis.

9.7 If the request relates to CCTV images of the requester and those images include other identifiable individuals, it may be necessary to obscure the images of the other individuals if providing their images to the requester would involve an unfair intrusion into their privacy or cause them unwarranted harm or distress. Where there is no such intrusion or harm, then it may not be necessary to obscure the other individuals' identities.

9.8 Always keep a record of what you have decided to do and your reasons for doing it.

10 How should the information be provided

10.1 The individual is entitled to be provided with a copy of his or her personal data.

10.2 We should aim to provide the information in digital form, redacted where appropriate.

11 Requests made by third parties on behalf of the individual

11.1 Occasionally we may receive a request for subject access by a third party (an 'agent') acting on behalf of an individual. These agents may include parents, guardians, legal representatives and those acting under a power of attorney or other legal authority. The agent must provide sufficient evidence that he or she is authorised to act on behalf of the individual for all such requests.

12 Exemptions to the right of subject access

12.1 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:

12.1.1 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.

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

12.1.2.1 education, training or employment of the individual;

12.1.2.2 appointment of the individual to any office; or

12.1.2.3 provision by the individual of any service

12.1.3 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:

12.1.3.1 'Advice privilege' covers confidential communications between ACEMAT and our lawyers where the dominant purpose of the communication is the seeking or giving of legal advice;

12.1.3.2 'Litigation privilege' covers any document which was created with the dominant purpose of being used in actual or anticipated litigation (eg 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 subject access request is received.

12.1.4 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 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.

12.1.5 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 HR is negotiating with an employee in order to agree the terms of a redundancy package and the employee makes a subject access request, HR 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.

13 Deleting personal data in the normal course of business

13.1 The information that we are required to supply in response to a subject access request must be supplied by reference to the data in question at the time the request was received. However, as we have 30 days in which to respond and we are generally unlikely to respond on the same day as we receive the request, we are allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data are supplied if such amendment or deletion would have been made regardless of the receipt of the subject access request.

13.2 We are, therefore, allowed to carry out regular housekeeping activities even if this means that we delete or amend personal data after the receipt of a subject access request. What we are not allowed to do is amend or delete data because we do not want to supply the data.

14 Consequences of failing to comply with a request

14.1 If we fail to comply with a subject access request or fail to provide access to all the personal data requested, or fail to respond within the 30-day time period, or the extensions, we will be in breach of the GDPR and the DPA. This may have several consequences:

14.1.1 the individual may complain to the Information Commissioner and this may lead the Commissioner to investigate the complaint. If we are found to be in breach, enforcement action could follow (which could include monetary penalties);

14.1.2 if an individual has suffered damage, or damage and distress, as a result of our breach of the GDPR and the DPA, he or she may take us to court and claim damages from us; and/or

14.1.3 a court may order us to comply with the subject access request if we are found not to have complied with our obligations under the GDPR.