AECC University College

Version: 1.0
Effective from: 01.03.2021
Procedure owner: Data Protection Officer

Subject Access Requests Policy & Procedure

1. Policy

1.1 Under data protection legislation an individual has the right (subject to certain exemptions) to access the information that an organisation holds about them. It helps individuals to understand how and why we are using their data, and check we are doing it lawfully. Accessing personal data in this way is known as making a Subject Access Request (SAR). AECC University College DPO oversees this procedure and supports colleagues (referred to deputy through this document) who receive and action SAR requests.

1.2 Subject access requests are different to requests submitted under Freedom of Information (FOI) legislation, which relate to information about the organisation itself. Further information can be found within the University Colleges Freedom of information Policy.

1.3 Any person wishing to access their personal data under the provisions of the General Data Protection Regulation and Data Protection Act 2018 should make a Subject Access Request (SAR).

1.4 An individual can make a SAR verbally or in writing, including on social media. A request is valid if it is clear that the individual is asking for their own personal data. An individual does not need to use a specific form of words, refer to legislation or direct the request to a specific contact.

1.5 The University College encourages individuals to use our SAR form. These are available for individuals to download from our website and available in print form from clinical departments.

1.6 An individual may ask a third party (e.g. a relative, friend or solicitor) to make a SAR on their behalf. Before responding, the DPO or deputy needs to be satisfied that the third party making the request is entitled to act on behalf of the individual. It is the third party's responsibility to provide evidence of their authority.

1.7 Before responding to a SAR for information held about a child, the DPO or their deputy must consider whether the child is mature enough to understand their rights. If the request is from a child and the DPO or deputy are confident they can understand their rights, we should usually respond directly to the child. We may, however, allow the parent or guardian to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child. If a child is competent, they may authorise someone else, other than a parent or guardian, to make a SAR on their behalf.

1.8 AECC UC must comply with a SAR without undue delay and at the latest within one month of receiving the request. This can be extended by a further two months if the request is complex or we have received a number of requests from the individual, e.g. other types of requests relating to individuals' rights.

1.9 If AECC UC processes a large amount of information about an individual, we are able to ask

them to specify the information or processing activities their request relates to, if it is not clear. The time limit for responding to the request is paused until we receive clarification, although we should supply any of the supplementary information we can do within one month.

1.10 AECC UC needs to be satisfied that we know the identity of the requester (or the person the request is made on behalf of). If we are unsure, we can ask for information to verify an individual's identity. The timescale for responding to a SAR does not begin until we have received the requested information. However, we should request ID documents promptly.

1.11 In most cases AECC UC cannot charge a fee to comply with a SAR. However, we can charge a 'reasonable fee' for the administrative costs of complying with a request if it is manifestly unfounded or excessive, or if an individual requests further copies of their data. Discussion with the DPO should take place before any charges are imposed.

1.12 The institution should make reasonable efforts to find and retrieve the requested information. However, we are not required to conduct searches that would be unreasonable or disproportionate to the importance of providing access to the information.

1.13 If an individual makes a request electronically, we should provide the information in a commonly used electronic format, unless the individual requests otherwise.

1.14 When deciding what format to use, we should consider both the circumstances of the particular request and whether the individual has the ability to access the data we provide in that format. It is good practice to establish the individual's preferred format prior to fulfilling their request. Alternatives can also include allowing the individual to access their data remotely and download a copy in an appropriate format.

1.15 If an individual asks, AECC UC can provide a verbal response to their SAR, provided that we have confirmed their identity by other means. We should keep a record of the date they made the request, the date we responded, details of who provided the information and what information was provided.

1.16 It is important that however the data is transferred to an individual it is done in a secure manner.

1.17 Where an exemption applies, we may refuse to provide all or some of the requested information, depending on the circumstances. We can also refuse to comply with a SAR if it is manifestly unfounded or manifestly excessive. See Appendix 1 for further examples of when refusal may be appropriate.

1.18 If we refuse to comply with a request, we must inform the individual of:

- the reasons why;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through the courts.

1.19 Where possible, AECC UC should consider whether it is possible to comply with the request without disclosing information that identifies another individual. If this is not possible, we do not have to comply with the request except where the other individual consents to the disclosure or it is reasonable to comply with the request without that individual's consent.

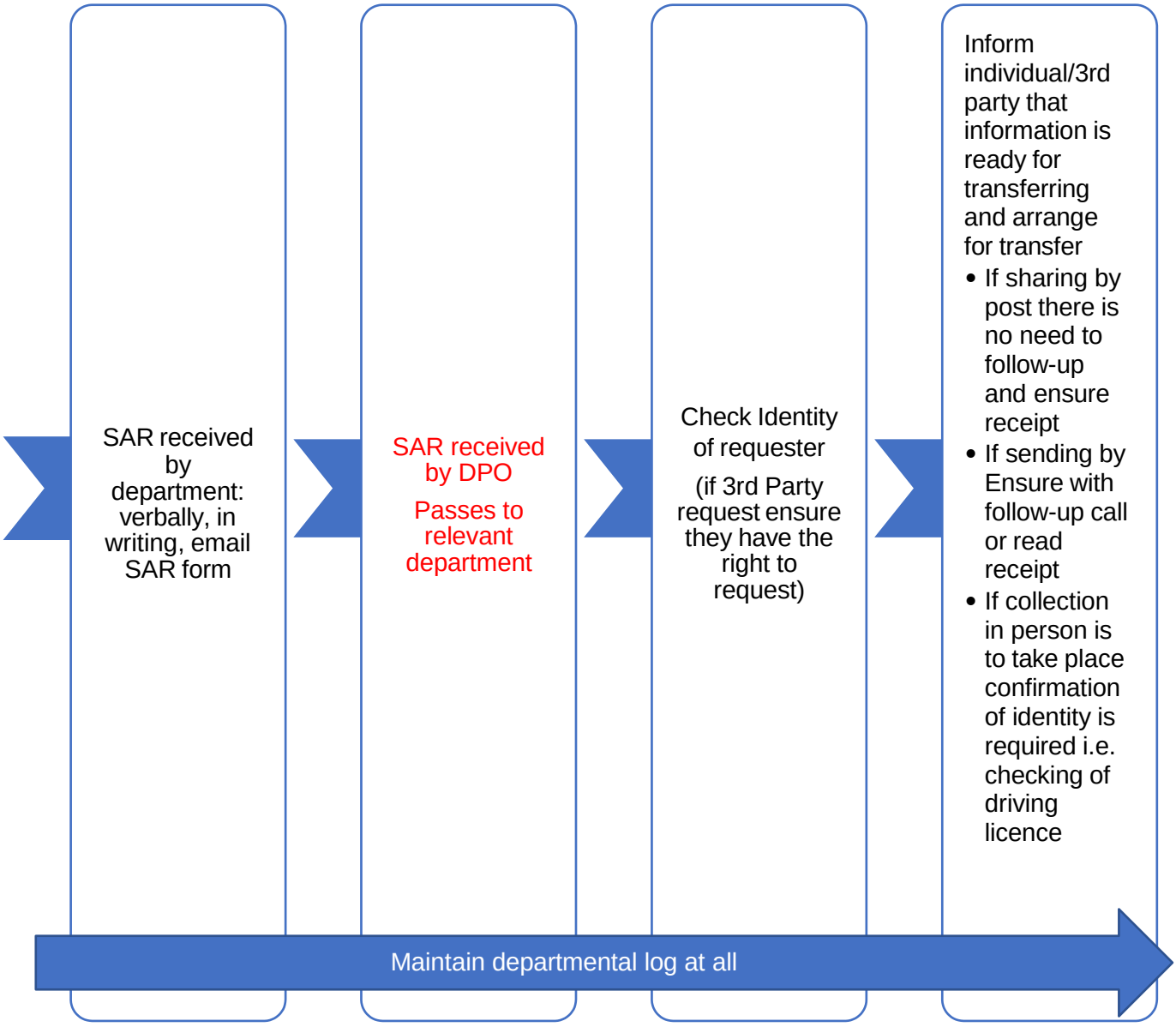
1.20 The institution needs to respond to the requester whether or not we decide to disclose information about a third party. We must be able to justify our decision to disclose or withhold information about a third party, so we should keep a record of what we decide and why.

1.21 AECC UC should be mindful that the ICO may take action against a controller or processor if they fail to comply with data protection legislation.

2. Procedure for Managing SARs

2.1 In most circumstances it is likely the department will receive the SAR request directly, in particular the below departments will receive request directly and will manage the request and will maintain a log of all actions. Prior to release of any documentation, oversight and sign-off must be sought by the relevant departmental clinical lead or manager.

Department	SAR departmental main contact
Clinic	Clinic Operations Manager (or deputy)
US Clinic	Manager – School of Radiology (or deputy)
MRI	Superintendent MRI Radiographer (or deputy)
Registry	Academic Registrar (or deputy)
HR	Head of People & Development (or deputy)



The DPO is always available to help support departments in the management of SARs Departments maintain their own logs and provide the DPO with a bi-annual report of the number of SAR requests and outcomes which the DPO adds to their central log record.

Appendix 1

Examples of possible reasons to refuse SAR's

- Crime and taxation: general
- Crime and taxation: risk assessment
- Legal professional privilege
- Functions designed to protect the public
- Regulatory functions relating to legal services, the health service and children's services
- Other regulatory functions
- Judicial appointments, independence and proceedings
- Journalism, academia, art and literature
- Research and statistics
- Archiving in the public interest
- Health, education and social work data
- Child abuse data
- Management information
- Negotiations with the requester
- Confidential references
- Exam scripts and exam marks
- Other exemptions

There are special rules and provisions about SARs and some categories of personal data, including;

- unstructured manual records;
- credit files;
- health data;
- educational data; and
- social work data

Version:	3.0
Approved by	SMG
Originator / Author	Data Protection Officer
Policy Owner	Data Protection Officer
Reference source	HE Exemplars
Date approved	March 2021
Effective from	March 2021
Review date	March 2024
Target	Staff
Policy location	SIP
Equality analysis	No direct impact, the policy provides for equality analysis to be undertaken as part of policy review. The policy provides for information to be made available in alternative formats as required, to make reasonable adjustments in line with the Equality Act 2010.