Subject Access Request (SAR) Policy

Version:	**1**
Dated:	**01/09/2023**
Last review	**May 26**
Next review	**May 28**
Document Owner:	**SIRO/FAB Manager**

Version	Approval	Date
V 1.0	Compliance Committee	
	Reviewed by change of SIRO to CEO	May 26

Contents:

1. INTRODUCTION:

Under the UK General Data Protection Regulation (UK GDPR), individuals have the right to discover and obtain a copy of any information that an organization holds about them. This right can be exercised through a Subject Access Request (SAR), which allows individuals to learn about the Personal Data held by an organization concerning themselves, the purpose for/length of, its retention, and any entities it is shared with.

2. PURPOSE:

This Policy and Procedure sets out how Age UK Wiltshire (AUKW) manages its SAR responsibilities in accordance with legal and regulatory obligations. This Policy sets out the minimum standards which must be complied with when handling a SAR.

3. SCOPE:

The Policy applies to all data subjects such as service users and employees who request access to personal information that is held by AUKW. It includes all personal data AUKW collects and uses whether it is held in electronic or paper format and includes voice recordings, imaging records, photographs and CCTV.

3.1 Definitions:

- **Data Subject:** Any Individual who AUKW holds personal data about.
- **Personal Data:** Information relating to a data subject, which is identifiable to said subject.
- **Regulatory Authority:** Information Commissioners Office (ICO).
- **SIRO:** Senior Information Risk Owner.
- **IAO:** Information Asset Owner.
- **Third Party Data:** Data that is obtained from external sources.

4. RESPONSIBILITIES:

4.1 Employees:

Service leads (as IAO's): may be involved in the process of locating and retrieving the personal data requested in the SAR, ensuring its accuracy and co-ordinating a response in compliance with regulatory authority guidelines as per the procedure below. They may also play a role in facilitating the organisation's ability to respond effectively to SARs by liaising with relevant departments/individuals who possess the requested personal data.

All Staff Members, Including Volunteers: Have a responsibility to recognise and report a SAR to Business Support.

Business Support: Receive the SAR request, validating the subject's identity if necessary. Respond to SAR requests within the month timeframe, unless a complex request.

5. PROCEDURE:

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

Any staff member who happens upon a request sends an email to business support at **business.support@ageukwiltshire.org.uk.** The email should include; **the name and date of birth of the requestor, the data that has been requested, and the date that the SAR was received.**

5.1. The data subject has the right to request:

- Access to/copies of their personal data
- Confirmation that their data is being processed
- The reason for processing their personal data
- Whether data will be shared with other organisations or people
- The data retention period

5.2 Third Party Data:

Most of the time we will redact or remove any information which doesn't relate to the person making the SAR. This is to avoid inappropriately disclosing information about other people.

The one exemption where SAR compliance is not mandatory is if it means revealing information which identifies another individual.

This does not apply if:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

This means that the decision to disclose information relating to a third party is done on a case-by-case basis. The decision falls on us and we should consider the data subjects right of access, but also the other individual's rights relating to their own personal data. If they have consented to having information about them disclosed, we should go ahead. If there is no such consent, it rests on our decision-making as to whether to disclose the information anyway.

5.3. Identification:

If there is uncertainty around the identity of the data subject, they must provide identification to evidence that they are the requestor or that they are a third party who has the right to make the request on behalf of another. It is noted that formal identification is only relevant when necessary and proportionate. Asking questions that only the subject would know the answer to, i.e. about their engagement with AUKW's services or appointments attended may be more appropriate.

5.4. Finances:

SARs will be dealt with free of charge, unless the request is unusually large, complex, or an individual requests further copies of their data. If this is the case (the decision will be made by Business Support) a reasonable fee may be charged. If a fee is charged, the one-month time limit does not begin until the fee is received.

If a request is manifestly unfounded or excessive, particularly where it is repetitive, it can be refused. Any decision to refuse a request will be made by Business Support and should a request be refused, the Data Subject will be informed of the reasons why it is refused and of their right to complain to the Regulatory Authority, within one month of receipt of the request.

5.6. Timeframe:

Data subjects can typically expect to receive their response as soon as possible but no longer than one month after receiving the request. By default, the response will be delivered via email, unless the requester has specified an alternative method such as postal mail or in-person collection. In cases where information is sent by post, it will be securely sealed and dispatched via recorded delivery to the address provided during the identity verification process.

If we need to validate the identity of the requestor, the timeframe begins upon verification of identity.

In situations where the request is complex, such as those coming from an employee or involving social care information, the legislation allows for a possible extension of up to two additional months. The data subject will be informed of this extension within one month of receiving their request, if not earlier, along with a clear explanation regarding the reasons for the extension.

Some factors that may add to the complexity of a request include:

- technical difficulties in retrieving the information – for example if the data is electronically archived;
- the request involving large volumes of particularly sensitive information;
- potential issues around disclosing information about a child to a legal guardian; and
- any specialist work involved in redacting information or communicating it in an accessible way.

5.7. Response:

Our response will include the requestors personal data, alongside our privacy information. ICO guidance states that the requestor has a right to know why their data is being held, how it was obtained, the retention period, who it will be shared with and how they can request a change or deletion.

The respondent must clearly mark the information in disclosure bundles to identify which requestor it needs to go to and identify that it is part of a SAR request. This will ensure that it is not mistaken for general paperwork. The bundle will be marked by a label with relevant information, such as: requestor name, date, and whether it is the requestor copy or AUKW's. This is to ensure accuracy. If the response is being sent via email, any personal information should be encrypted where appropriate.

5.8. Retention:

All requests received in any part of the AUKW must be forwarded to Business Support for recording. A copy of the information sent will be retained for two years, unless there is a legal basis to retain for longer.

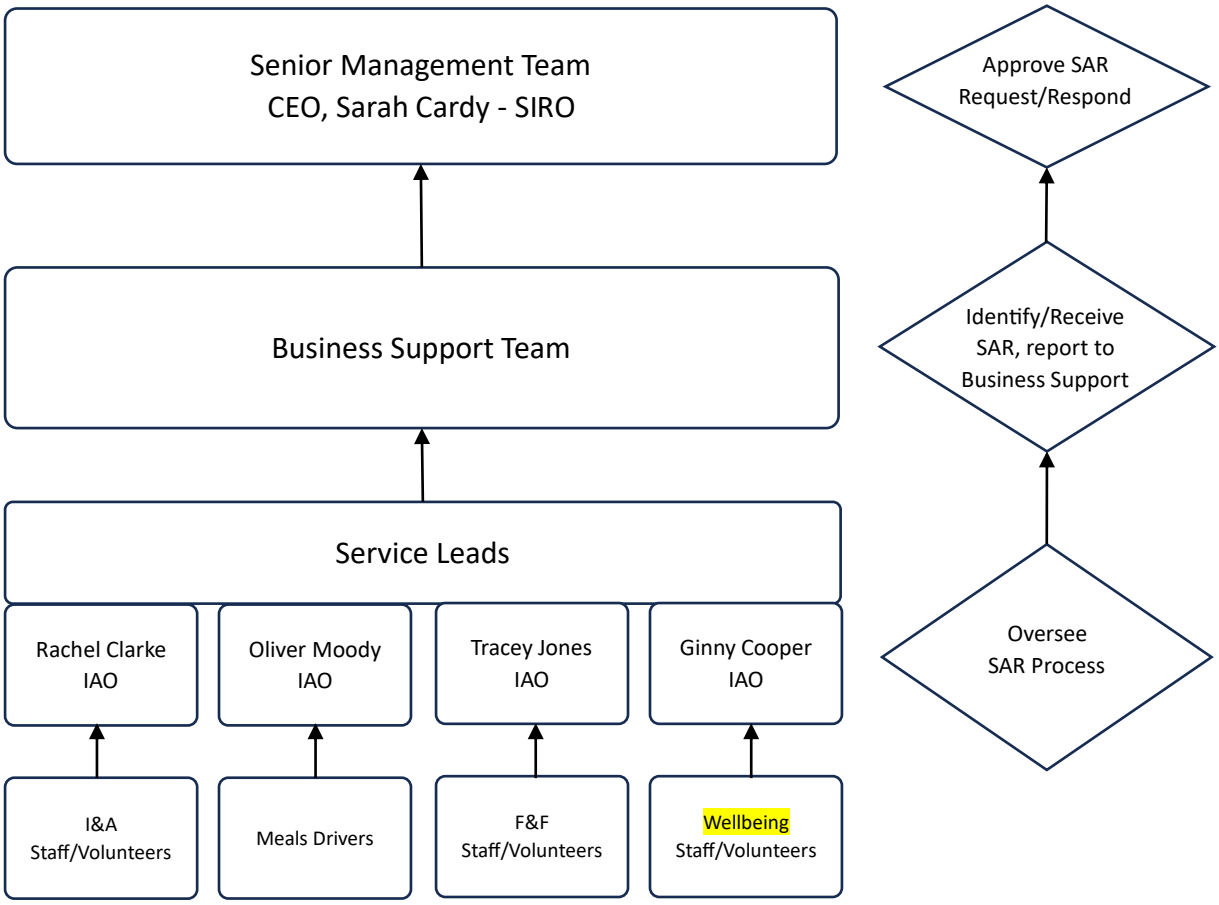
A copy of the information sent will be retained for two years by the department concerned as required by the Corporate Retention and Disposal Schedule, unless there is a legal basis to retain for longer.

Staff members must alert business support of the SAR via email, including the client's name and DOB and a description of the data requested.

Business Support will then:

1. Verify the identity of the requestor if unsure.
2. Check our information records with information provided by requestor to ensure we can locate the information.
3. Issue a response to the data subject containing the information requested which is safely encrypted, I.e. a password protected email or a clearly marked disclosure bundle. A requestor must be notified if their response will be delayed or if we cannot locate the information requested.
4. Update the SARs Log, populating the following information: date received, response due and received by, responsible staff member, reason for extension (if given), rejections, exemptions + redactions, identity checks completed/fee requested + method of communication/delivery.

- **SAR REPORTING CHAIN:**



6. TRAINING AND AWARENESS:

All staff are required to undertake regular data protection and information security training in order to ensure compliance.

AUKW's SAR Training Objectives:

- Increase awareness and understanding of SAR regulations, policies, and procedures.
- Enable staff, volunteers, and stakeholders to handle SARs effectively.

Training Content:

- Overview of SARs and their importance.
- How to spot a SAR, where to escalate it.
- Familiarization with the ICO guidance and data protection legislation.
- Understanding the process of handling SARs, including documentation and timelines.
- Understand exemptions and redactions.

7. ACCOUNTABILITY:

Policy Requirement	Procedures	Accountable
Procedures implemented and communicated	AUKW adhere to a SAR procedure which is regularly reviewed. Policy kept centrally to ensure awareness and accessibility.	All AUKW Staff, SLT to raise awareness.
Designated team handle SARs	A team within AUKW are allocated SAR responsibility. This includes review and authorisation of redactions and exemptions.	Business Support.
Staff handling SARs have appropriate training	All employees are provided with advice on recognising and responding to a SAR.	All AUKW Staff and SLT to raise awareness and signpost policies and training.
Data Subjects identity validated where necessary	Team assessing the request ensure ID/Security Question/Verification docs for SARs where we are unsure of the requestor's identity.	Business Support
SAR Data is sent securely	Emails containing SAR information should be encrypted /password protected. Physical copies are securely sealed and sent via recorded delivery.	Business Support
Documentation	Number of SARs received documented in SAR Log. Response time and complaints also documented. Requests responded to within a month, unless a complex request is made.	Business Support

8. COMPLAINTS:

If data subjects are dissatisfied with the response to their Subject Access Request (SAR), they have the right to request a review. In respect to the transparency principle of GDPR, we will inform the data subject of this right.

To complain, an individual can contact Business Support detailing the nature of their complaint.

The review will then be conducted by Business Support/ The SIRO who will communicate their findings to the data subject and address any concerns identified. In case the data subject remains unsatisfied, they retain the right to escalate the matter to the Information Commissioner for a further assessment of compliance.

Further information regarding the SAR process can be found at:

https://ico.org.uk/

Telephone: 0303 123 1113

Fax: 01625 524510

Live Chat: https://ico.org.uk/global/contact-us/live-chat

9: REDACTIONS:

AUKW will redact any information about individuals not relating to the SAR.

10. REVIEW:

This policy will be subject to review every 2 years. An earlier review will be undertaken if recommended by the Trustee Board in response to exceptional circumstances, such as relevant changes in legislation/guidance.