Subject Access Request Procedure

Index

Purpose

The purpose of this procedure is to outline the steps that must be taken in the event that a service user initiates a Subject Access Request (SAR) with Age UK Sutton.

Background

Under the General Data Protection Regulation, individuals have the right to request a copy of all information an organisation holds on them. This information must be provided free of charge (unless the request can be deemed as "manifestly unfounded or excessive, or if the request is made repeatedly") , must be acknowledged within 30 calendar days of a valid request being made and provided without undue delay.

Responsibilities

The Systems and Insight Manager is responsible for the management and completion of subject access request. All staff are expected to be able to recognise when a valid request has been made and are responsible for informing the Systems and Insight Manager at the earliest possible opportunity.

Section 1: Procedure

1.1 **Request**

A standard form is available for use when a SAR is made, however use of this form is not mandatory. Details of the request should be forwarded to the Systems and Insight Manager who manages SARs.

1.2 **Verification**

The Systems and Insight Manager will verify that all of the details required to complete a SAR have been provided. Depending on the type of information that is being requested, the requestor's identity may need to be verified to ensure they have the right to access the information they are requesting. In order to verify the requestor's identity, the following documentation will be requested:

1.2.1 Confirmation of name (1 of the following)

- Full driving licence
- Passport
- Birth certificate
- Marriage certificate

1.2.2 Confirmation of address (1 of the following)

- Utility bill
- Bank statement
- Credit card statement
- Benefit confirmation / letter from local authority / government

1.2.3 Confirmation that a third party can access the records (if appropriate)

- Health and Welfare Lasting Power of Attorney
- Court of Protection Order appointing you as a personal deputy for the personal welfare of the data subject
- Signed declaration from the Data Subject themselves

1.2.4 During the verification process the individual will also be asked what format they would prefer the information to be presented in and their preferred method of receipt (either via email of post, depending on preferred format).

1.3 Record SAR information

All instances of SARs will be initially recorded in the Subject Access Request Log. Once the individual's identity and right to access the information has been established, information about the request will also be recorded on the individual's record on Charitylog (including the date of the initial request and any specific information the individual is requesting).

1.4 Process Request

The individuals records on all systems that they are stored in should be exported using each systems export record functionality. Different individuals may have information stored on one of more of the following systems:

1.4.1 Clients

- Charitylog
- PeoplePlanner

1.4.2 Volunteers

- Charitylog
- Google Drive

1.4.3 Staff

- Charitylog
- People Planner
- Google Drive

1.4.4 A log of all information that is exported and where the information came from should be recorded on both the Subject Access Request Log and the Charitylog SAR record. Care should be taken to not disclose any information that could relate to currently ongoing

investigations covering issues such as fraud or any information that could potential identify an individual other than the subject of the Subject Access Request.

1.5 Provide Data

The information requested by the individual should be provided to them in the format that they have requested, with the following provision for each method of delivery:

1.5.1 **Email:** Information should be collected in an encrypted, password protected archive file, along with instructions on how to decrypt the archive (See Section 3 for details on how to encrypt files). The password for the file should be noted in the Subject Access Request Log and provided to the individual via a telephone call. The password should not be recorded on the Charitylog SAR record.

1.5.2 **Post:** The delivery address should be confirmed with the individual before sending via the post. Information should be posted using Signed For Next Day Delivery, with tracking numbers recorded on the Subject Access Request Log.

1.5.3 Details of the delivery method and the date sent should be recorded on both the Subject Access Request Log and the Charitylog SAR record. The standard letter (Subject Access Request Cover Letter.docx) should also be included with letters and **Section 4 – Email template** should be used when sending information via email.

1.6 Request Closure

Once the information has been sent to the individual, the Subject Access Request Log and the Charitylog SAR should be reviewed to ensure the details of the request have been recorded accurately. The request should then be closed on both the Subject Access Request Log and the Charitylog SAR record, using the date that the information was checked as the closure date.

1.7 Time Scales for Subject Access Request Completion

Below is an outline of the timescales involved in the administration of a Subject Access Request:

Before identity verification	
Day 0	• Initial Subject Access Request received by office
Day 0 – Day 1	• Systems & Insight Manager to be informed that a request has been made
Day 1 – Day 3	• Systems & Insight Manager to contact client, confirm the process and the next steps to be completed, including documents required for identity verification. • Letter of confirmation to be sent to client

	• Request to be logged in Subject Access Request Log
Day 3+	• Subject Access Requests can only be progressed once the identity of the requestor and their right to access the information has been confirmed •
After identity verification	
Day 1	• Once the request has been verified, create record on Charitylog and update Subject Access Request Log • Letter confirming verification and outlining what happens next to be sent out
Day 1 – Day 7	• Review systems to confirm where individuals information is being processed • Update both logs to record which systems have been reviewed
Day 8 – Day 11	• Information collated in to format requested • Information reviewed to ensure information relating to other individuals is removed (if present)
Day 12	• Final checks to ensure information provided complies with original request
Day 13	• Information sent to client in required format • Both logs to be updated with dates and details of information that has been sent • Request closed after final checks on logs have been completed

Section 2: Retention Periods

2.1 The retention periods for each part of the Subject Access Request Process are as follows:

- Subject Access Request Log – 3 years
- Subject Access Request Charitylog Record – 3 years
- Details of documentation used for verification – 1 year
- Copy of Personal Information Requested – 1 year (original information to be retained in line with other relevant retention periods and statutory/contractual requirements)

2.2 All data relating to a Subject Access Request is to be anonymised or, if anonymization is not appropriate, deleted, in line with the above timescales.

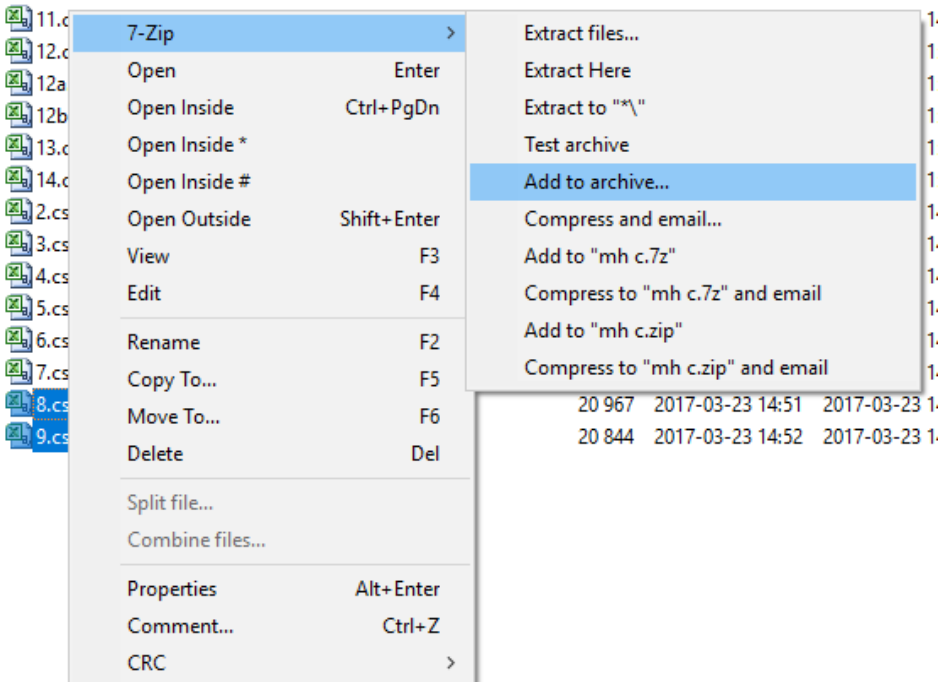
Section 3: Document encryption instructions

3.1 Age UK Sutton uses AES-256 encryption through the use of 7zip to encrypt files for transfers to external individuals in response to Subject Access Requests. To encrypt a file (or group of files), follow these steps:

3.1.1 **Open 7zip**
Press the Windows key and type 7zip (if 7zip is not displayed in the search results, navigate to the folder called 7zip on the Program List and select 7zip File Manager)

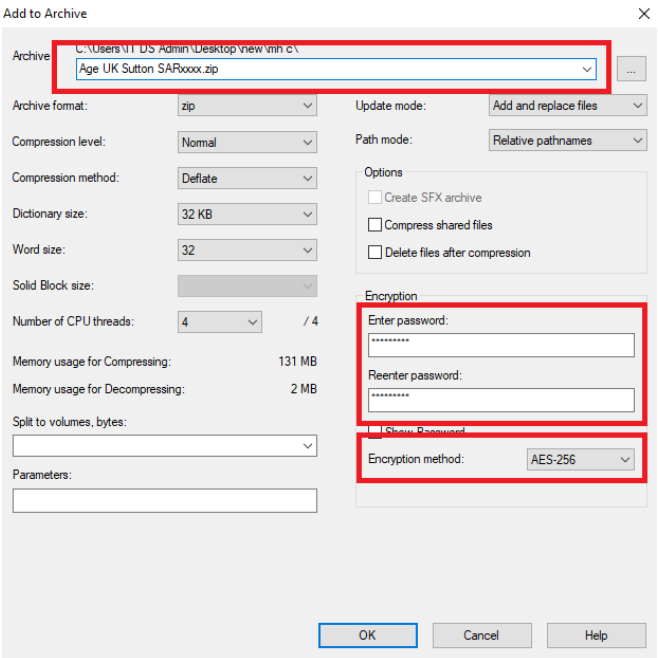
3.1.2 Select the files to be encrypted

Files can be encrypted individually however if there are multiple files to be sent it is better to encrypt them collectively. Navigate in the 7zip window to the file(s) you want to encrypt, select them (using the CTRL key if selecting more than one file) and right click on one of the selected files, then hover over 7zip and select Add to archive



3.1.3 Encryption settings

The settings for encryption should be set as follows:



The name should be the next available name in sequence based on previous entries in the Subject Access Request Log. The password should be set using Age UK Sutton's password policy (see the IT Policy for more information) and the Encryption method should be set to AES-256. Click **OK** and the files will be collected into an encrypted archive in the same folder that the files are in

3.1.4 Send to requestor

The encrypted archive, along with the decryption instructions, should then be emailed to the requestor. The encrypted archive should be stored in the Subject Access Request folder and the password should be stored in the Subject Access Request Log.

Section 4: Email template

Dear Sir/Madam

General Data Protection Regulation
Subject Access Request, Reference Number: [number].

In reply to your application to access data in respect of the following:-
[details of request, e.g. pass type and number, employee information]

I attach a copy of all the data which satisfies your request.

The attached file is password protected. You should have received a call from us already with your password, however if you haven't please contact the office 0208 770 5360.

If you have any queries regarding this matter please contact [Co-ordinator's name] who is the designated person dealing with this enquiry. Please quote the reference number provided above in all of your correspondence.

Yours faithfully

Section 5: Associated documents

- Privacy Standard.pdf
- Subject Access Request Log.xlsx
- Subject Access Request Form.pdf
- Subject Access Request Cover Letter.docx