1. **Introduction**

This policy documents the requirements for the management of Subject Access Requests (SARs)

- Definition of SAR
- Identifying and notifying a SAR
- Responding to a SAR
- Completion of a SAR

2. **Objective**

To provide a clear process for responding to SARs in accordance with the rights of individuals and the requirements of the GDPR:

- Ensuring that all staff, volunteers, temporary workers and contractors understand how to recognise a SAR and what to do if a SAR is received
- Defining and appropriately implementing critical controls
- Ensuring compliance with applicable regulatory and statutory requirements

3. **Scope**

This policy applies to all IoF staff, contractors, volunteers and temporary workers.

Breaches of this policy will be taken very seriously by the IoF and may result in disciplinary proceedings, including possible dismissal (in accordance with applicable laws and/or contract of employment).
4. **Definitions**

4.1 **Subject Access Request**

In addition to being provided with a copy of personal data held, all individuals have a right to the following:

- The purposes of the processing
- The categories of personal data concerned
- The recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular to recipients in third countries or international organisations
- The envisaged period for which the personal data will be stored, or the criteria used to determine that period
- Rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
- Lodge a complaint with a supervisory authority (ICO/Fundraising Regulator)
- Where the personal data are not collected from the data subject, any available information as to their source
- Know the existence of automated decision making including profiling (referred to in Article 22(1) and (4) of GDPR) and at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject
- Know, where personal data are transferred to a third country or to an international organisation, the appropriate safeguards relating to the transfer

4.2 **Data**

- Information processed by electronic means
- Information recorded with the intention that it should be processed by electronic means
- Information which is held in a non-automated format which forms part of, or is intended to form part of a filing system
- Information that forms part of an ‘accessible record’

4.3 **Filing System**

A structured set of personal data which are accessible according to specific criteria.

4.4 **Personal Data**

Any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, ID number, location data, online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

4.5 **Third Party Data**

Personal data belonging to an individual who is not the subject of the SAR.
4.6 **Exemptions**

Conditions which enable withholding particular information in certain circumstances.

4.7 **Data Protection Team (DPT)**

Team of individuals at IoF who have extensive knowledge of SAR requirements under GDPR and are fully trained to enable a SAR to be fulfilled.

4.8 **Business Improvement Lead (BIL)**

Individual with responsibility for ensuring IoF’s data protection compliance.

4.9 **Individuals**

For the purpose of this document, all IoF staff, volunteers, temporary workers, contactors and consultants working on behalf of the IoF will be referred to as individuals.

4.10 **Third Party**

An individual or body which is not the data subject.

4.11 **Recipient**

Person receiving the SAR.

4.12 **Compliance Team**

IoF staff who have access to the Compliance inbox.

4.13 **Lead**

Member of the DPT responsible for collating all SAR information and responding to the request.

5. **Policy**

All individuals must be able to identify a SAR and understand the process they need to undergo to comply with this.

This policy and procedure looks at handling a Subject Access Request where an individual requests copies of information held about them or asks for minor updates/corrections to their data. Requests for other rights are handled in separate sub policies (see “Individual Rights” policy for the right to erasure, data portability and restricting processing).

5.1 to 5.2.3 below outline the processes to be followed by individuals receiving a SAR. Section 6 describes the procedure to be followed by the BIL and DPT.
5.1 **Identify the request**

There is no specific wording required to ask for a SAR nor a specific format in which requests have to be made. Therefore all individuals need to be alert to requests which may be made by letter, email, social media, phone or face to face.

5.1.1 **Amendment Requests Received from Data Subject**

Where a data subject just wishes to confirm information held (e.g. what phone number do you have for me?), they should be directed to their registration page on the IoF website where applicable and told they can view and update their information upon access.

In cases where this is not applicable, individuals should confirm they are communicating directly with the data subject before divulging any information. If the data subject requires amendments to their data (e.g. their email address has changed), the individual should facilitate these amendments and ensure that all relevant departments and groups within the IoF are also provided with the amendments.

5.1.2 **Amendments to Organisational and Corporate Members**

Organisational and Corporate members provide the IoF with key contacts. Where a request is received to change the contact details or remove/add a contact, this can be facilitated by individuals so long as they confirm that the request was authorised by a senior manager of that member organisation.

5.1.3 **Amendments Requested by a Third Party**

Except in the case of 5.1.2 above, individuals should not update information where the request is made by someone other than the data subject and should ask that the data subject contacts them direct. Where the data subject is unavailable, the individual should direct the third party to contact the BIL by email to compliance@institute-of-fundraising.org.uk including the words Data Protection in the subject heading.

5.2 **Subject Access Request – Initial Enquiry**

If the request is for information exceeding a simple change of details and/or falls into the categories listed in the definition of a SAR (see 4.1 above), the recipient must take as much information as possible regarding the request and complete a SAR form (see Appendix A). As a minimum the following information must be collected:

- Source of request (e.g. letter, email, social media, telephone, face to face)
- Date of request
- Name of data subject
- Contact details of data subject (ideally including email address and telephone number)
- Name of person making the request (if not data subject)
- Contact details of person making the request (if not data subject) including:
  - Email address
5.2.1 **Subject Access Request Received Outside of London Head Office**

Within 24 hours of receiving the SAR or no later than the first business day after receipt, a copy of the completed form must be passed to the BIL and DPT using one of the following:

**Using Secure Data Transfer**

Where secure data transfer is available, this facility must be used.

Within 24 hours of receiving the SAR and no later than the first business day after receipt, send an email marked ‘High Priority’ and with the subject Heading “SAR Request” to [compliance@institute-of-fundraising.org.uk](mailto:compliance@institute-of-fundraising.org.uk).

The email should say the following:

“I received a SAR on [date]. I have completed the SAR Form and a copy was transferred to [electronic location].”

A member of the DPT will be in touch with you to confirm safe receipt of the form and you may then shred the original.

**By Post**

Where there is no secure data transfer available, a copy of the form must be sent by first class post to:

Compliance – Urgent
Institute of Fundraising
Charter House
13-15 Carteret Street
London
SW1H 9DJ

Only post a copy and keep the original in a secure place.

Within 24 hours of receiving the SAR or no later than the first business day after receipt, send an email marked ‘High Priority’ and with the subject Heading “SAR Request” to [compliance@institute-of-fundraising.org.uk](mailto:compliance@institute-of-fundraising.org.uk).

The email should say the following:

“I received a SAR on [date]. I have completed the SAR form and a copy was sent to Charter House by first class post on [date].”

A member of the DPT will be in touch to confirm receipt of your email and further to confirm receipt of the SAR form.
5.2.2 **Subject Access Requested Received by Charter House Individuals**

When a Charter House individual receives a SAR they must complete the SAR Form and hand this to a member of the DPT within 24 hours of receiving the request.

The individual must send an email marked high priority to and with the subject heading “SAR Request” to compliance@institute-of-fundraising.org.uk.

The email should say the following:

“I received a SAR on [date]. I have completed the SAR form and passed this to [name] on [date].”

5.2.3 **Individuals Making a Subject Access Request**

Individuals working on behalf of the IoF are entitled to make their own SAR. To facilitate this they should complete a SAR form and follow the relevant process above.

6.0 **Fulfilling SAR**

6.1 **Compliance Inbox**

At least 2 members of the DPT including the BIL must have access to the Compliance Inbox at all times.

6.2 **Receipt of Notification of SAR**

Upon receipt of a SAR notification in the Compliance Inbox, the DPT must be informed immediately by a member of the Compliance Team.

A list of active members of the DPT will be held by the BIL and Compliance Team.

The BIL will confirm receipt of the notification with the SAR recipient within 24 hours of receipt of the notification. Where the BIL is not available, another member of the DPT will confirm receipt of the notification letting all members of the DPT know that this has been done.

6.3 **Receipt of SAR Form**

Upon receipt of a SAR form, the DPT must be informed immediately by a member of the Compliance Team.

The BIL will confirm receipt of the form with the SAR recipient with 24 hours of receiving the SAR form. Where the BIL is not available, another member of the DPT will confirm receipt of the SAR form letting all members of the DPT know that this has been done.
6.4 **Electing a Lead**

Dependent on the nature of the SAR and resourcing available, the DPT will elect a Lead to collate the information required to fulfil the SAR and to prepare the response. The Lead must be elected within 72 hours of receiving the completed SAR form.

Where there is a conflict of interest because the data subject is a member of the DPT, the data subject will be asked to step down from the DPT in this instance.

6.5 **Creating a SAR Log**

Upon election, the Lead will create a SAR Log. This will be in electronic format and only accessible by members of the DPT. See Appendix B for example SAR Log.

As a minimum the SAR Log must contain the following information:

Name and contact details of data subject
Relationship of data subject with IoF
Date request first received
Date SAR information must be provided
Information requested by data subject
Name of Lead
Confirmation of identity of data subject or authorisation to request information if request is from third party

All actions taken in relation to fulfilling the SAR must be included in the log.

6.6 **Confirming Request is a SAR**

If there is any doubt whether or not the request is a SAR or is a routine enquiry, the Lead must clarify the position with the individual. This should be done in writing by email or letter and include a request for any further information to complete the identity checks (see 5.3.7 below).

6.7 **Identity Checks**

i. **Data Subject**

Where the request is made by the data subject and there is any doubt that it is the data subject making the request, the Lead may request a copy of a passport or birth certificate and utility bill for evidence. Such requests must be made without delay.

If the request is made from a recognised email or other address or telephone number belonging to the data subject, or is made in person and the individual is known to the IoF, the IoF will in most cases consider this sufficient evidence but can request additional information such as membership number where relevant.
ii. **Requests from Third Parties**

Where a third party is acting on behalf of the data subject, the third party must provide written authority to make the request or provide proof of power of attorney. Such requests must be made without delay.

Requests for further identity checks must be made without delay upon receipt of the SAR and should not prevent commencement of information gathering. Requests for identity checks must explain that the SAR will not proceed until the information has been received. The Lead should adjust the SAR log to demonstrate when the request was sent and the new completion date for fulfilling the SAR.

6.8 **Further Information Required**

Where the scope of the request is unclear or additional information is required to locate the information requested, the Lead may request further information. This could include:

- The relationship with the IoF (e.g. member, delegate at events, former employee, employee, supplier, etc.)
- Suggesting parameters for searches or asking whether there is specific information they are looking for
- Approximate dates and senders of requested emails
- When that person had dealings with the IoF and any particular people they communicated with

The individual does not have to respond to this request and is within their right to ask for all information held about them.

6.9 **When no Personal Data is found**

If the IoF does not hold any personal data about the individual, the Lead must write to the individual as soon as possible to explain this.

6.10 **Locating Requested Information**

Based on the SAR, the DPT should agree locations to search for the information and this must be documented giving reasons for inclusion and exclusion of any possible sources.

The Lead can assign other members of the DPT to assist in locating requested information and also call upon members of other departments and groups to assist.

The Lead must ensure that where data is held in electronic format, all appropriate locations have been searched including networks, websites, stand-alone devices and archives.

The Lead must also ensure that no personal data is held by processors acting on behalf of the IoF is overlooked and in particular should consider including the following in the search:
Communicator  
Survey Monkey  
MailChimp  
Eventbrite  
Groups  
Trust Networks  
CharityJobs  
Civil Society

Where data is stored in hard copy, only structured filing systems need to be searched (including archives). This includes information which is intended for said filing systems but not yet filed.

The Lead and DPT must take into consideration any information which is likely to be changed between the date of receiving the request and its fulfilment. This includes data retention and back up policies applied.

Where there is no time to access information prior to a routine data retention programme being run, this must be documented and explained in full when fulfilling the request.

6.11 Assessing Information

For each piece of information collected, the DPT need to go through identifying the following:

Is there personal data relating to the data subject?  
Is all of it personal data? If no, only include information relevant to the data subject  
Is there any third party personal data? If yes, review in accordance with 5.3.12 below and carry out the balance test  
Are there any special circumstance? (e.g. litigation)  
Do any exemptions apply? (See 5.3.14 below)

6.12 Third Party Personal Data

The DPT must identify all information which identifies third party personal data.

Where possible and where this does not impact the rights of the individual requesting the information, third party personal data should be redacted.

Electronically this would be by the deletion of the third party personal data. In hard copy this may be through copying the hard copy with the third party personal data blanked out.

In some instances, it may still be possible to identify the third party individual. In these instances the DPT must carry out a balance test:

   a. Establish if there is any duty of confidentiality owed by the IoF and if so, decide whether or not consent should be sought. The reasoning must be documented

   b. Assess the impact on the third party in disclosing their personal data
c. Weigh the need to preserve confidentiality for the third party against the requestor’s right to access information

Where consent is not sought from or given by the third party, the DPT must get sign off from two directors of the IoF before providing third party information.

In any case, the third party must be told if the information is to be disclosed.

6.13 Special Circumstances

The Lead must ensure that there are no special circumstances prevailing which may have an impact on the way the SAR is dealt with (such as litigation).

6.14 Exemptions

The DPT must check against the exemptions allowed in prevailing legislation at the time of the SAR. Where an exemption is to be relied upon, this must be detailed to the requestor of the SAR.

In some cases, the DPT should seek further legal advice before applying an exemption.

6.15 Acronyms and Codes

Where acronyms and/or codes are contained in the information being supplied, the DPT must ensure that these are clearly explained.

6.16 Response and Review

The Lead must ensure that all actions in the SAR Checklist have been completed (see Appendix C for SAR Checklist).

The Lead should compile a response to the requester including the following information:

- The categories of data held
- The processing applied and conditions of processing relied upon
- A list of information provided
- Reasons for any redaction
- Reasons for withholding information (including third party personal data and exemptions)
- Explanations of any codes or acronyms contained in the information

The DPT including at least one director of the IoF must review and agree the response and all information prior to sending.

6.17 Sending the Information

Information should be sent electronically. Where this is not possible, alternatives should be discussed and agreed with the requester.

6.18 Storing the SAR
All information relating to the SAR must be kept for a 12 month period following completion of the SAR. The SAR information must be stored in a folder with access limited to the DPT.

All hard copy information must be filed and referenced to the electronic SAR folder. Hard copy information must be stored in a secure filing cabinet.

6.19 **Repeat Requests**

If a repeat request is received, the DPT should decide whether they consider a reasonable interval of time has lapsed since the original request. In particular in these deliberations, the DPT should consider:

i. the nature of the data – including whether it is particularly sensitive

ii. the purposes of the processing – is the processing likely to cause detriment (harm) to the individual; and

iii. how often the data is altered – if information is unlikely to have changed between requests the DPT may consider not repeating the request and instead informing the requester that the information is unlikely to have changed.

The outcomes of these deliberations should be documented.

If the requests are considered to be manifestly unfounded or excessive, in particular because of their repetitive character, the DPT may refuse the request or charge a reasonable fee for repeating the request.

Where it is considered that a reasonable length of time has lapsed, the Lead may request that only new information is provided, but has to provide all information if this option is refused by the data subject.

7.0 **Documents Referred**

This document refers to the prevailing SAR exemptions published by the ICO and prevailing data protection legislation.

8.0 **Appendices**

Appendix A – SAR Form
Appendix B – SAR Log
Appendix C – SAR Checklist
Appendix A – Subject Access Request Form

IMPORTANT: Read all the instructions below
Upon receipt of a Subject Access Request, please complete this form and send an email with the subject marked as “SAR Request” to compliance@institute-of-fundraising.org.uk within 24 hours of receiving the request or on the first business day after receipt of the SAR latest. The email should be marked high priority and just state that you have received a SAR, the date it was received and that you have forwarded the SAR form (refer to SAR policy for information on sending the SAR form). Please do not email this form as it contains personal data.

Subject Access Request Form

Date request received: __________

Name of person receiving request: ___________________________________________________________

Email address of person receiving request: ________________________________________________

Phone number of person receiving request: _______________________________________________

How was request made (please circle): Letter / Email / Social Media / Phone / Face to Face

Name of Data Subject: _________________________________________________________________

Address: __________________________________________________________________________

________________________________________________________________________________

Email Address: ____________________________________________________________________

Phone number: ____________________________________________________________________

Circle the category which best describes the relationship between the IoF and the Data Subject:
IoF Staff / IoF Volunteer / Temporary Worker (IoF) / Consultant (IoF) / Contractor (IoF) / IoF Member
Other (please describe) _______________________________________________________________

Was the request received from the data subject? Yes ☐ No ☐
If No, please give details of person/body making the request:

Name: ________________________________________________________________

Address: ______________________________________________________________

________________________________________________________________________

Email Address: ____________________________________________________________

Phone number: ___________________________________________________________________

Nature of enquiry (please provide as much detail as you about the request, e.g. what information has been asked for, if this is a complaint, etc.)
## Appendix B – Example SAR Log

<table>
<thead>
<tr>
<th>Action</th>
<th>Date</th>
<th>Method</th>
<th>Actioned by</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date request received</td>
<td>01/03/2018</td>
<td>Phone</td>
<td>Peter Brown</td>
<td></td>
</tr>
<tr>
<td>Date SAR form received</td>
<td>03/03/2018</td>
<td>Transfer</td>
<td>Peter Brown</td>
<td></td>
</tr>
<tr>
<td>Receipt of SAR acknowledged to recipient</td>
<td>03/03/2018</td>
<td>Email</td>
<td>John Smith</td>
<td></td>
</tr>
<tr>
<td>Receipt of SAR acknowledged to data subject</td>
<td>03/03/2018</td>
<td>Email</td>
<td>John Smith</td>
<td></td>
</tr>
<tr>
<td>Copy of passport and utility bill requested</td>
<td>03/03/2018</td>
<td>Email</td>
<td>John Smith</td>
<td></td>
</tr>
<tr>
<td>Additional information requested</td>
<td>03/03/2018</td>
<td>Email</td>
<td>John Smith</td>
<td>Relationship to IoF, people dealt with and timescales</td>
</tr>
<tr>
<td>DPT Informed</td>
<td>03/03/2018</td>
<td>Email</td>
<td>John Smith</td>
<td></td>
</tr>
<tr>
<td>Electronic SAR folder created</td>
<td>03/03/2018</td>
<td>Email</td>
<td>John Smith</td>
<td>G:/Data Protection/SAR/001 Mrs Suzanne Jones</td>
</tr>
<tr>
<td>DPT meeting to start scoping information</td>
<td>05/03/2018</td>
<td>Email</td>
<td>John Smith</td>
<td>Meeting minuted and minutes stored in SAR folder</td>
</tr>
</tbody>
</table>
Appendix C – SAR Checklist

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the request a SAR or a routine enquiry to the organisation? If there is any doubt, clarify the position with the individual</td>
<td></td>
</tr>
<tr>
<td>Has a record been made of the date on which a request was made, any period when the ‘clock stopped’ (e.g. when verifying the identity of the requester) and when the response is due?</td>
<td></td>
</tr>
<tr>
<td>Has the process to verify the identity of the requester been followed?</td>
<td></td>
</tr>
<tr>
<td>Is the scope of the request clear or is any additional information required to locate the information requested and to deal with the request?</td>
<td></td>
</tr>
<tr>
<td>Are personal data about the requester held by the organisation? If not, has the requester been informed?</td>
<td></td>
</tr>
<tr>
<td>Are personal data relating to the requester stored in manual and/or electronic form?</td>
<td></td>
</tr>
<tr>
<td>If held in manual form, is the information held in a structured filing system?</td>
<td></td>
</tr>
<tr>
<td>For electronic records, have all appropriate locations been searched, including networks, stand-alone devices, archives?</td>
<td></td>
</tr>
<tr>
<td>Have service provided which may be processing the personal data been identified? If so, have they been notified of the request and asked to provide the relevant information (or asked to deal with the request, if required to do so under the terms of their contract)?</td>
<td></td>
</tr>
<tr>
<td>Is any of the information which is subject of the request due to be changed between the date of the request and the provision of the information?</td>
<td></td>
</tr>
<tr>
<td>Is any third party personal data included within the request? If so, have the internal procedures been followed with regard to assessing whether such information may be disclosed (including taking into account any express refusal of consent to disclosure or duty of confidentiality owed to the third party in question)?</td>
<td></td>
</tr>
<tr>
<td>Are there any special circumstances pertaining to the request (such as current litigation) which may impact on the way the request is dealt with?</td>
<td></td>
</tr>
<tr>
<td>Have all relevant exemptions been considered? If so, has legal advice been obtained to ensure that they are being applied correctly (e.g. if relying upon legal privilege as an exemption)?</td>
<td></td>
</tr>
<tr>
<td>Have the reasons for the application of exemptions been documented, including the basis for any refusal to release third party personal data?</td>
<td></td>
</tr>
<tr>
<td>Have exemptions been applied consistently?</td>
<td></td>
</tr>
<tr>
<td>Does the application of exemptions involve the redaction of any information? If so have internal policies regarding appropriate methods of redaction been followed?</td>
<td></td>
</tr>
<tr>
<td>Does the information being disclosed include any codes or acronyms which require explanation?</td>
<td></td>
</tr>
<tr>
<td>Is the nature of the information such that it is not possible to provide the information in permanent form on the basis of disproportionate effort? If so, what steps have been taken for the information to be provided in alternative form (such as by inspection)?</td>
<td></td>
</tr>
<tr>
<td>Has the response been reviewed internally in accordance with relevant procedures before being sent to the individual?</td>
<td></td>
</tr>
</tbody>
</table>