A4 Data Protection Policy

Appendix 2 Subject Access Request Procedure

1.Introduction

1.1. GFS processes personal information about a range of people including; current and former employees, members, volunteers, donors, girls and young, women, parents, suppliers, and consultants.

1.2. Under the provisions of the General Data Protection Regulations, (GDPR) 2018 and Data Protection Act (DPA)1998, a data subject (individual) has a right to be informed about the personal information an organisation holds about them, why it is held and for how long.

1.3. This procedural guide sets out the process for managing a subject access request within GFS. It should be read in conjunction with the GFS Data Protection Policy and Data Protection Breach Procedure.

2.Subject Access Request

2.1. A Subject Access Request (SAR) is a written request submitted by or on behalf of an individual requesting information about their personal data and how it is being processed.

2.2. A request may not use or specify the term *subject access request* but it should be clear from the content that the individual is seeking information held about their personal data.

3.Personal Data

3.1. Personal Data is any information that relates to a living individual (the 'data subject') and

- enables that person to be identified from the data and
- any other information which is held by or likely to come into the possession of the organisation.

3.2. This includes;

- Paper: Information held in manual form including hand written notes or printouts from an electronic format
- Electronic: emails, databases, spreadsheets and reports
- Photographs: ID cards

- Publications
- Web pages

3.3. It also includes information held on any mobile device (phone, laptop, tablet etc.) and those associated with online identifiers such as Internet Protocol (IP) addresses and cookie identifiers.

4. Subject Access Rights

4.1. The General Data Protection Regulation 2018, entitles an individual to request;

- Information about what personal data is being processed about them
- Given a description of the personal data, why it is being processed, whether it will be given to any other organisation or people,
- Given a copy of the personal data, and
- Given details of the source of the data
- A right to prevent processing likely to cause them substantial damage or distress or significantly to prejudice their rights and freedoms;
- A right to prevent processing for the purposes of direct marketing
- A right to stop automated decision-taking
- A right to have incorrect data rectified, blocked, erased or destroyed

4.2. GFS requires a SAR to be submitted in writing by the individual or someone acting on their behalf. GFS has prepared a template for this purpose however, may also accept a SAR presented in other formats including;

- Email
- Text
- GFS social media accounts including Facebook or Twitter

4.3. GFS will ensure training is in place to support identification and processing of all SARs. However, if there is any doubt about the status of a request for information please forward details to the data manager at head office operations@girlsfriendlysociety.org.uk

4.4. The requester does not need to provide a detailed explanation or justification for their request however they may be required to clarify the type of information sought and the time period to support retrieval of data.

5. Requests for Information about a Child

5.1. GFS works with girls and young women and recognises that even if a child is too young to understand the legal implications of a subject access request, the information about that child or young person belongs to them. GFS may therefore inform the child/young person that a request has been made for access to information about their personal data.

6. Requests from a child/young person

6.1. A SAR may be submitted by a child or young person. Before responding the data manager will consider whether the child is mature enough to understand (in broad terms) their rights and ensure the process is accessible to that child or

young person. The ICO recommends a child aged 13 years and above is able to submit a request for their personal information.

7. Third Party Requests for information about a child

7.1. A SAR for information about a child may be submitted by a parent or guardian of a child. It may also be submitted by other third party agencies such as the police. Such requests must be made in writing, explaining what personal data is required and the reasons why it is required.

7.2. All requests of this nature must be sent to the data manager at GFS Head Office where it will be dealt with.

8. Data Manager

8.1 The Operations Manager will act as the data manager. The post holder is responsible for ensuring compliance with GFS Data Protection policies; including administration of SARs, Breach Procedures, risk management, record keeping, and registering the organisation with the Information Commissioners Office.

9. Time Limits

9.1. GFS will respond to a SAR without delay and undertakes to resolve requests within the statutory period of **1 month**.

10. Fees

10.1. GFS may in exceptional cases charge an administrative fee for dealing with a SAR and may not respond until this has been paid. The maximum fee payable is £10.00.

11. Responding to a Subject Access Request

1. A subject access request may be received in a local group, branch, at a GFS event or head office.
   Upon receipt, the staff member, trustee, volunteer or other GFS representative should forward this to the data manager at GFS Head Office without delay.
2. If you are in receipt of a SAR. You should explain what will happen to their request and provide contact details for the GFS data manager at Head Office.
3. No personal data should be released without notifying the data manager and confirming the identity of the requester.
4. The data manager will be responsible for confirming the identity of the applicant.
5. The data manager may contact a staff/volunteer, trustee or person acting on behalf of GFS as part of the ID verification process and may request information that enables confirmation of;
   a. Name
   b. Date of Birth
   c. Address
   d. Location of group
   e. Nature of relationship with GFS e.g. volunteer, staff, parent.

f. Any other significant identifier.

6. The data manager may contact the person submitting the SAR for more details of the request.
7. Following verification of identity and clarification of the information required (e.g. specific time period, event etc.) the data manager will contact identified respondents to confirm the deadline by which information is required.
8. All information held must be given to the data manager. (This may include searching files, emails, personal computer drives, mobile phone records etc. (wherever possible this should be sent to the data manager via email).
9. You may discover information that does not reflect positively on individuals or the organisation. For example, you may find documents that show policies and procedures are not being followed. **You must not destroy or refuse to disclose these documents.**
10. Not all personal information may be liable to disclosure. The data manager will complete screening (see below) and may contact you if clarification or further information is required.
11. The data manager will write to the applicant enclosing all information eligible for disclosure and/or explain why the information requested cannot be disclosed.

12.Data Manager Responsibilities

12.1. Check that the Subject Access Request is valid.

GFS will subject to the above (section 7) only send personal information to the data subject and will take reasonable steps to check the validity of the SAR. The data manager may contact the local group/branch or line manager as a part of the verification process and will also contact the individual to;

a. Verify identity by phone

To verify the identity of the data subject GFS will ask a series of questions based on information we hold and will record answers for the purpose of complying with the SAR request.

b. Verify identity in writing

GFS may write to the individual and ask them to send a photocopy or proof of identity documents such as passport or driving license and proof of address.

c. Third Party requests

If a request is made by a third party e.g. solicitor, it is their responsibility to obtain the correct permission from the data subject (individual) before approaching GFS. We will also require proof of identity.

All third party requests must be submitted in writing.

If the information requested relates to a child GFS will consider;

- Proof age and whether the child is mature enough to understand their rights; (the minimum age will be 13;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information;
- any views the child or young person has on whether their parents should have access to information about them.

13. Check that the individual ('data subject') has provided all relevant information.

13.1.A SAR may not include sufficient detail necessary to enable GFS to respond to it.

13.2. The data manager may write to the requester to provide additional information that may narrow the scope or clarify the information requested e.g. name of group, dates, event etc.

14. Record the SAR and calculate the target date for response

14.1. The data manager will record the date SAR is received and when identity has been verified. This will inform the deadline by which a response to the requester will be made.

14.2. The deadline (**1 month**) for a response starts following verification of identity and where appropriate any fee due is made.

15. Find relevant information

15.1. The data manager will contact the relevant staff, volunteers, data processors, trustees etc. informing them of the deadline and format of information required.

15.2. If you hold personal data; you may be required to search paper based and electronic files, registers, emails, texts, social media, personal computer drives, mobile phone and archived materials.

a. **Personal Devices**
   GFS provides mobile phones to eligible staff members. Staff may not hold information about customers, contacts or other employees on their own personal devices.
b. If a staff member holds personal data on their own personal device this falls within the scope of any SAR received and information must be provided on request to the Data manager.
c. **Emails**
   The contents of emails stored on GFS devices falls within the scope of a SAR.

15.3. A request from the data manager for information related to a SAR must be given priority and deadline dates adhered to.

15.4. If unsure about any aspect of the information requested or have any difficulties associated with the provision of information you must contact the data manager.

15.5. The information provider should not attempt to screen information sent to the data manager nor should any attempt be made to delete or otherwise destroy information relating to the SAR.

15.6. All reasonable costs associated with provision of the information requested will be reimbursed in accordance with GFS financial procedures.

16. Evaluate the information obtained.

16.1.GFS recognises not all personal data may be liable for disclosure. Once the information has been collected the data manager will examine it in detail to establish if it should be disclosed. The data manager may seek external advice in determining disclosure.

16.2. The data manager will;

- Check the information provided is about the individual (data subject)
- Screen out duplicate copies. (e.g. the last email in a chain will be printed if the previous email is included within it).
- If a record was created by a staff member, volunteer or trustee in a private capacity GFS will seek their consent and only in exceptional circumstances would there be a justification to disclose the information without their consent.
- Remove data about other individuals.

16.3. Where a document contains personal data about a number of individuals including the data subject that information should be provided to the data manager who will then consider;

- Whether the disclosure requires the consent of information that identifies a third party;
- Has the third party given their consent
- Whether it is reasonable to disclose the information without the third party consent
- Confidentiality

17. The SAR response

17.1. The data manager will respond to each SAR even if, following investigation, it does not hold any personal data. All communications related to a SAR must be directed to the data manager who is responsible for providing the response;

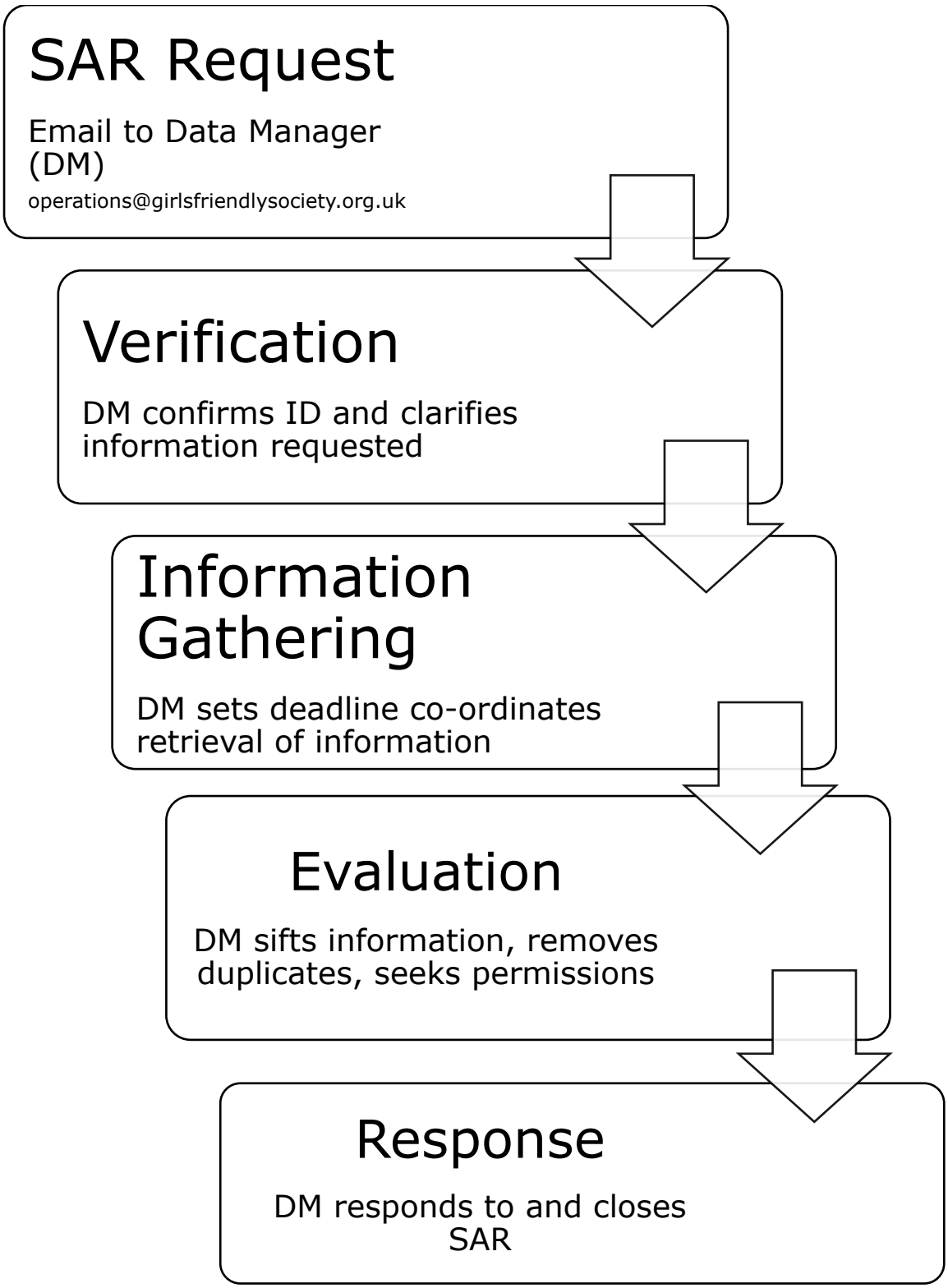
17.2. The response may include;

- whether any personal data is being processed;

- a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people; and
- the source of the data (if known).

18. Closing the SAR record

18.1. When the request has been completed the data manager will update the log and close the SAR record.


SAR Request
Email to Data Manager (DM)
operations@girlsfriendlysociety.org.uk
Verification
DM confirms ID and clarifies information requested
Information Gathering
DM sets deadline co-ordinates retrieval of information
Evaluation
DM sifts information, removes duplicates, seeks permissions
Response
DM responds to and closes SAR