	Gasóga na hÉireann / Scouting Ireland			
	No.	Issued	Amended	Next Review Date
	SI-DP-G01	20 MAR 2026	NA	MAR 2027
	Category: Data Protection			
Guidelines for Scout Groups on managing Subject Access Requests				

Related Documents
SI-DP-01 Scouting Ireland Data Protection Policy
SI-DP-02 Scouting Ireland Subject Access Request Policy

Revision Schedule		
Revision	Date	Description
1.0	20MAR2026	This is the first version of these guidelines

Guidelines for Scout Groups – Subject Access Requests

See **SI-DP-02 Scouting Ireland Subject Access Request Policy** regarding details on Subject Access Requests (SARS) and GDPR.

Table of Contents

Table of Contents.....	2
1. Introduction	3
2. Subject Access Process.....	3
1. Subject Access Request is received.....	3
2. Group Leader / Designee Acknowledges Request.....	4
3. Group Leader / Designee confirms ID and date of reply	4
4. Collate the necessary data.....	4
5. Redactions and Exclusions	5
6. Information Provision	5
7. Resolve issues	6
8. Retention of Subject Access Request.....	6
3. Support.....	6
4. Key Takeaways	6
5. Templates.....	7

1. Introduction

This document is to provide guidance and templates for volunteer-led Scout Groups on how to handle Subject Access Requests (SARs).

As Scout Groups are both independent and joint (with Scouting Ireland National office) data controllers of personal data they collect and store about their members, they would respond directly to a Subject Access Request from a member or Parent / Guardian of a member in relation to personal data held at Group Level.

Examples of personal data held by groups are:

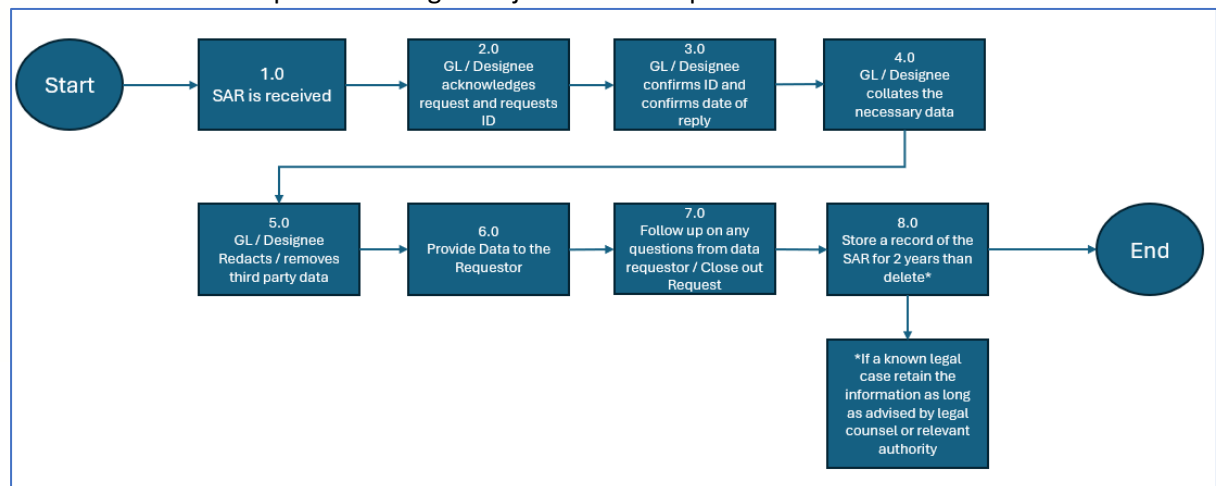
- Application forms
- Activity Consent forms
- Sign in sheets
- Medication record forms
- Message content (E.g. WhatsApp / Text / Email)
- Meeting minutes which directly / indirectly identify an individual
- Photographs etc.

Any questions or for support on how to manage a SAR please reach out to Scouting Irelands Data Protection Officer for support (dataprotection@scouts.ie).

It is suggested that one volunteer is assigned the role of data protection point of contact within the group. This could be any member of group council it does not have to be the Group Leader.

2. Subject Access Process

Below outlines the steps to handling a Subject Access Request.



1. Subject Access Request is received

- A request for personal data could be in any format and does not need to be in an official manner.

- It could be in writing via email, message, or a verbal request to any volunteer within the Scout Group.
- It may also come via Scouting Irelands Data Protection Officer (DPO) who will forward onto the Group leader for review.
- If the requestor (Data Subject) is requesting data held at National Level (i.e. anything outside of the Group level) then please forward it to the DPO dataprotection@scouts.ie.
- All SARS must be actioned within 1 calendar month so please do not delay in actioning.

2. Group Leader / Designee Acknowledges Request

- Confirm to the Data Subject that their request has been received – ideally in writing, so you have this on record. (See Template 1)
- To ensure you are releasing data to the appropriate person you can ask them to confirm their ID
- Usually this is a request for the data subjects Date of Birth, phone number and emergency contact name in which you can compare against the Membership Management System (MMS).
- Just to note if you already know this person and are satisfied the request is coming from them then there is no need to confirm ID but please take note of this.

3. Group Leader / Designee confirms ID and date of reply

- Once you are satisfied with the person's ID confirm back to them that you will go ahead and process the request and will do so within 1 calendar month of the request. (See Template 2)
- You have **1 calendar month** to provide all the requested data.
- In the event the amount of personal data requested is excessive or complex, you may extend the timeframe to two additional calendar months, but you must let the requestor know within the first month of the request.

4. Collate the necessary data

- Ensure you are only providing personal data **related to the request** and only data created **up to the date of request**.
- Search your electronic and paper files - see Subject Access Request Checklist to help guide you on your search
- Request to other relevant Group Council / volunteers for anything they might have
- Copies of the personal data should be provided rather than the original.
- If there is a request for data specific to a Safeguarding case, please reach out to Safeguarding and the DPO to work with them on fulfilling the request.
- WhatsApp, Text messages and emails are privy to Subject Access Requests – Please note only messages sent in Scouting capacity and only the messages that relate to the data subject are provided in response to a SAR.
- Photographs of the data subject are also personal data, so if a request for all data is received, then don't forget to include these too (ensuring other individuals in the photos are cropped out).
- If there are emails or messages from or to the data subject – let them know you have this data and ask in your reply to them if they want this to be included also.

5. Redactions and Exclusions

Redactions – removing third party data or content not related to the Data

Subject:

- When responding to a SAR – you **only need to provide personal data and content about the data subject** – you do not need to provide personal data of other individuals unless it will not affect their rights and freedoms.
- Example there is an email which references the data subject and two other volunteers names and the content of the email is discussing them helping out on a weekly section meeting – very unlikely this will affect the other individuals if shared with the requestor, so this is acceptable to leave in – however if any doubt always redact the data.
- When redacting third party data please ensure it is not visible, in most cases if black marker is used on a paper form the data is still visible.
- Adobe Pro has redacting functionality, if you ever need support in redacting data you can always reach out to National Office DPO (dataprotection@scouts.ie) for support.
- Always **avoid sharing other youth members** personal data.
 - Example a sign in sheet is to be provided as part of the SAR – remove the other youth members data – this is not needed in the response.
- **Safeguarding data / Data provided in confidence**
 - If a request comes in relating to Safeguarding, then liase with the Safeguarding team and notify the DPO.
 - If part of the request is looking for something that has been given in confidence this must be reviewed on a case-by-case basis. Reach out to the DPO who can help with this.

Exclusions:

Under data protection law, not all information is required to be disclosed under a SAR. The following are examples of (but not limited to) information that falls outside of the scope of a SAR.

- **Non-personal data** such as Scout Group policies, procedures, or general operational documents that do not relate specifically to the requestor.
- **Duplicate records:** Where the same information appears multiple times across different documents. You may consolidate or limit duplicate copies to avoid unnecessary duplication in response.
- **Anonymised data** where individuals cannot be identified.

6. Information Provision

- Once all personal data has been gathered, reviewed and redacted create an inventory of the documents (See Template 3).
- In the inventory note anything that was not included but could be related to the Data Subject and why you are not including this for transparency purposes.
 - Example: Messages to and from the data subject as they would already have this

- Example: X Data excluded due to it being provided in confidence and could potentially disclose another individual and have an effect on their rights and freedom.
- Share this data with the requestor via a secure method (See Email Template 4), examples are as follows:
 - Link to file in your Scout Groups electronic filing system where only they and the person providing the data will have access to (ensuring this does not give the requestor access to other data for the group)
 - If sending anything via post do so by registered post
 - If none of the above are possible the DPO can support, you in providing this information electronically via SharePoint.

7. Resolve issues

Reply to any follow up questions / issues and close out once complete.

8. Retention of Subject Access Request

- Save a copy of all communications in relation to the SAR as well as copies of the data provided – suggested retention is 2 years from the time the SAR is completed to allow time for follow ups / disputes and resolutions.
- Delete once this timeframe has passed unless there is a legal reason / request to retain it for longer.
- Ensure limited access to this SAR is applied.

3. Support

If you receive a Subject Access Request and require support and / or guidance at any stage please reach out to the Data Protection Officer. You can reach the Data Protection Officer via email dataprotection@scouts.ie or by calling National Office during office hours on 01 495 6300. Reminder, you have 30 days to fulfill a SAR so the sooner you request support the better.

4. Key Takeaways

- 1. Recognise a Subject Access Request**
 - Understand what constitutes a SAR and be able to identify when one has been made
- 2. Identify Personal data held by your group**
 - Be aware of the types of personal data your group holds, including photographs, and know where this data is stored
- 3. Remove Third-Party Data**
 - Ensure that any personal data relating to individuals other than the requestor is excluded, unless it is relevant and permissible to share.
- 4. Safeguarding related requests**
 - If the request involves safeguarding concerns, contact both the Safeguarding team and the Data Protection Office (DPO) for advice before proceeding.
- 5. Understand the Response Timeframe**

- SARs must be responded to within 30 calendar days of receipt
- 6. Prepare a Data Inventory**
 - Include a clear inventory of the data being provided, along with notes explaining any redactions or exclusions.
 - 7. Retain SAR Records**
 - Keep a copy of all communications and the data provided for two years from date of SAR Closure.
 - 8. Seek Support When Needed**
 - Contact Scouting Ireland's Data Protection Officer (DPO) for assistance or clarification at any stage of the process.

5. Templates

The following templates are designed to support you in creating responses to the requestor. You can amend as you see fit.

Template 1 – Email Acknowledging and requesting ID

Dear [Name],

I am writing to let you know that we have received your Subject Access Request (SAR) sent to [Group Leader of NNNN Scout Group] on [Date]. Your request has been logged.

In order to process this SAR we are required to verify your identity to ensure the safe and proper release of personal data.

Please reply with the following information in order that we may confirm it against the details held about you on our Membership Management System:

- Phone number
- Emergency Contact
- Date of birth

Once we have verified your identity we will be in a position to respond to your request.

Yours sincerely

Template 2 – Confirms ID and Confirms date of reply

Dear [Name]

Thank you for verifying your identity. I can confirm that we will now process your Subject Access Request as soon as possible, and certainly within one month of your request.

You will hear back from us by [add in date 30 days from time of request] at the latest. If there are any delays or questions related to your request, we will be in contact sooner.

Yours sincerely

Template 3 – Data Inventory

The information included in here is for examples only.

Document Title	Description	Categories of Personal data Processed	Purpose of Processing	Format	Redacted comments
Group Council Meeting Minutes 01 June 2025	Meeting Minutes from the Group Council meeting on the 01 June 2025	Personal Data (Identification data)	Example: To record attendance, participation, and decision-making accountability during council meetings	Word Doc	Comments about what is being shared if needed – include here what you have redacted / removed example “Removed third party data as not related to the data subject “or “Removed additional content as this was not related to the data subject”.
		Membership Data		Email	
		Sensitive Data		WhatsApp Message	
		Contact Data			
		Training Data			

Examples of Categories and examples of personal data included in these categories

- **Personal data (Identification):** First name, last name, Date of Birth. Gender, Photograph(s)
- **Membership data:** Membership number, Membership position, type, start and end dates, event registrations / attendances, vetting completed dates,
- **Emergency Contact Data:** Emergency Contact Name, Emergency Contact Number, Emergency Contact Address
- **Contact Data:** Email, Phone, Address
- **Training Data:** Safeguarding Training, other training attendance
- **Sensitive Data:** Health data, political views, sex life or sexual orientation, Racial or ethnic origin, political opinions, Religious or philosophical beliefs, trade union membership, genetic data, biometric data,

Template 4 – Email to requestor when sending the data – amend as required depending on how you are sharing the data – the below is based on using SharePoint.

Dear [NAME]

In response to your subject access request dated DDMMYYYY, I am pleased to enclose relevant documents via [SharePoint folder].

This is a secure folder only you and I have access to. I will send the link shortly, if you have not received it within the next hour, please let me know.

I will delete this folder on DDMMYYYY so please download what you need before then. Included is an inventory to outline what has been provided and any relevant comments / redactions made.

You will see in some of the documents there are redactions made as this is related to third party personal data and has been redacted to ensure we do not adversely affect the rights and freedoms of others (Article 15(4)) and / or is content not related to you / **[insert data subject name]**.

To confirm no automated decision making or profiling has been carried out using your personal data.

If the information we hold about you / **[insert Data subject name]** is inaccurate and you would like us to rectify it, please let us know.

In certain circumstances you can also ask us to erase the information or restrict the use of the information. You can also object to how your information is being used. If you contact us requesting erasure or restriction, please explain the reason for your request.

If you are dissatisfied with this response, please let us know so that we can address any concerns or you can also make a complaint to the following:

- Scouting Irelands Data Protection Officer dataprotection@scouts.ie
- Data Protection Commissioners Office. Information on how to do this is available at [Raising a concern with the commission | Data Protection Commissioner](#).

Many Thanks