Data Protection Policy

Introduction - Privacy and data protection as a key policy for Scouting

The Scout Association's commitment to protecting privacy and data protection is a key policy for Scouting. This key policy underpins both this Data Protection Policy and other associated policies used by Rosyth District Scouts. It is important to note that Rosyth District Scouts are responsible for the data it processes when managing the activity of the District. Individual Scout Groups are directly responsible for any personal data they process and must therefore ensure that they are aware of their responsibilities under the law.

1. Purpose of this Data Protection policy and what it covers

This policy sets out Rosyth District Scout's approach to protecting personal data and explains your rights in relation to how we may process personal data. More detail in respect of how we process and protect your data is provided below, in particular in section 5.

Rosyth District Scouts ("We" in this document) are a Scottish Charity registered with the Office of the Scottish Charity Regulator (OSCR). Our Scottish Charity Number is SC008476.

We may update this policy from time to time in minor respects, although we will make sure that any substantial or significant changes are clear. If you have any queries about anything set out in this policy or about your own rights, please email rosythdc@yahoo.co.uk

2. Some Important Definitions

'We' means Rosyth District Scouts
'ICO' is the Information Commissioner's Office, the body responsible for enforcing data protection legislation within the UK and the regulatory authority for the purposes of the GDPR
'**Personal Data**' is defined in section 3
'Processing' means all aspects of handling personal data, for example collecting, recording, keeping, storing, sharing, archiving, deleting and destroying it.
'Data Controller' means anyone (a person, people, public authority, agency or any other body) which, on its own or with others, decides the purposes and methods of processing personal data. We are a data controller insofar as we process personal data in the ways described in this policy.
'**Data processor'** means anyone who processes personal data under the data controller's instructions, for example a service provider. We act as a data processor in certain circumstances.
'**Subject Access Request'** is a request for personal data that an organisation may hold about an individual. This request can be extended to include deletion, rectification and restriction of processing.
'**Compass**' is The Scout Association's web-based membership system. Local Scouting must comply with the Data Protection Act 1998 and the GDPR when using Scouts Scotland's Membership System known as Compass.
'Online Scout Manager' is a third party web-based application used to manage youth membership records and badge and award progress. Local Scouting must comply with the Data Protection Act 1998 and the GDPR when using Scouts Scotland's Membership System known as Compass.

3. What is personal data?

Personal data means any information about an identified or identifiable person. For example, an individual's home address, personal (home and mobile) phone numbers and email addresses, occupation, and so on are personal data. Some categories of personal data are recognised as being particularly sensitive ("sensitive personal data"). These include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic and biometric information, and data concerning a person's sex life or sexual orientation.

4. How does data protection apply to local Scouting?

Data protection legislation applies to all data controllers regardless of whether they are charities or small organisations. It applies to local Scouting in the same way as it does to other organisations. Scout Districts and Scout Groups are created and run as independent charities and insofar as they collect and store personal data about members and young people, for example, they are data controllers and must adhere to the law.

5. What type of personal data do we collect and why?

5.1 Members

We benefit from the service of a large number of adult members giving their time to Scouting at both District and Scout Group levels and a larger number of youth members who take part in the programmes that we offer. We may hold personal data (including sensitive personal data) about members on our membership database and other platforms. We believe it is important to be open and transparent about how we will use your personal data.

Information we may hold about you includes the following:

- name and contact details
- length and periods of service (and absence from service)
- details of training you receive
- details of your experience, qualifications, occupation, skills and any awards you have received
- details of Scouting events and activities you have taken part in
- details of next of kin
- age/date of birth
- details of any health conditions
- details of disclosure checks
- any complaints we have received about the member
- race or ethnic background and native languages
- religion
- photograph
- nationality

We need this information to communicate with you and to carry out any necessary checks to make sure that you can work with young people. We also have a responsibility to keep information about you, both during your membership and afterwards (due to our safeguarding responsibilities and to

help us if you leave or re-join). Much of this information is collected from the member joining forms.

5.2 Donors

We benefit from donations from members of the public who support our work, and we hold personal data about these donors so that we can process donations and tell donors how they can support us further. In addition to the information listed in 5.1, we may also hold information about eligibility to approve gift aid

6. Conditions for collecting personal data

6.1 Keeping to the law

We must keep to the law when processing personal data. To achieve this, we have to meet at least one of the following conditions:

- you have to give (or have given) your permission for us to use your information for one or more specific purposes
- we need to process the information to meet the terms of any contract you have entered into
- processing the information is necessary to keep to our legal obligations as data controller
- processing the information is necessary to protect your vital interests
- processing the information is necessary for tasks in the public interest or for us as the data controller to carry out our responsibilities
- processing the information is necessary for our legitimate interests (see below)

Also, information must be:

- processed fairly and lawfully
- collected for specified, clear and legitimate purposes
- adequate, relevant and limited to what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- processed securely

6.2 Information that we share

We may have to share your personal data within appropriate levels of The Scout Association, as long as this is necessary and directly related to your role within Scouting. We do not share personal data with companies, organisations and people outside the Association, unless one of the following applies.

- We have clear permission from you to do so.
- If we have to supply information to others (for example purchasing travel insurance) for processing on our behalf. We do this if we are asked and to make sure that they are keeping to the GDPR and have appropriate confidentiality and security measures in place.
- For safeguarding young people or for other legal reasons.

7. Keeping personal data secure

Everyone who handles personal data must make sure it is secure to protect against unlawful or unauthorised processing and accidental loss or damage. We take appropriate steps to make sure we keep all personal data secure, and we make all of our members aware of these steps. In most cases, personal data must be stored in appropriate systems and encrypted when necessary. The following is general guidance for everyone within Scouting, including members in local Scouting.

- You must only store personal data on networks, drives or files that are password protected and regularly backed up.
- You must have proper entry-control systems in place, and you must report any stranger seen in entry-controlled areas.
- You must keep paper records containing personal data secure. If you need to move paper records, you must do this strictly in line with data protection rules and procedures.
- You must not download personal data to mobile devices such USB sticks unless necessary. Access to this information must be password protected and the information deleted immediately after use.
- You must keep all personal data secure when travelling.
- Personal data relating to members must usually only be stored on the membership database or other specific databases, which have appropriate security in place.
- When sending larger amounts of personal data by post, you should use registered mail or a courier. Any devices must be encrypted.
- When sending personal data by email this must be appropriately authenticated and password protected. Do not send financial or sensitive information by email unless it is encrypted.
- You should not share your passwords with anyone.
- Different rights of access should be allocated to users depending on their need to access personal or confidential information. You should not have access to personal or confidential information unless you need it to carry out your role.
- Before sharing personal data with other people or organisations, you must ensure that they are GDPR compliant.
- In the event that you detect or suspect a breach, you must follow your defined breach response process.

All members must undertake The Scout Association's training on data protection.

8. Responsibilities

We expect our members to keep to the guidelines as set out in our Data Protection Policy and under ICO and GDPR guidance when they are using or processing personal data and other confidential or sensitive information as set out clearly below.

8.1 District Executive

Our District Executive has overall responsibility for Rosyth District Scouts and for making sure that we keep to legal requirements, including data protection legislation. Our District Commissioner, District Chair and the District Team are responsible for making sure we keep to these requirements across the District.

8.2 Data Protection Officer (DPO) or equivalent role holder

Rosyth District Scouts Executive Committee are responsible for ensuring the organisation is monitoring compliance with GDPR and other Data Protection laws, our data protection policies, awareness-raising, training, and audits. Scout Groups should consider doing similar. The Data Protection Officer is responsible for:

- making sure that this data protection policy is up to date
- advising you on data protection issues
- dealing with complaints about how we use personal and sensitive personal data reporting to the ICO if we do not keep to any regulations or legislation

8.4 Members and Scout Groups

We expect you to keep to data protection legislation and this data protection policy, and to follow the relevant rules set out in our Policy, Organisation and Rules (POR).

The local executive committee (trustees of local Scout Groups) has overall responsibility for keeping to data protection regulations.

As part of your data protection duties, you should report urgently (to your local manager or the executive committee) any instance where the rules on how we handle personal data are broken (or might be broken).

9. Data Retention

We may keep information for different periods for different purposes as required by law or best practice. Individual parts of the District include these periods in their processes. We make sure we store this in line with our Data Retention Policy.

As far as membership information is concerned, to make sure of continuity (for example if you leave and then re-join) and to carry out our legal responsibilities relating to safeguarding young people, we keep your membership information throughout your membership and after it ends, and we make sure we store it securely.

Only those members who need membership information to carry out their role have access to that information.

10. Rights to accessing and updating personal data

Under data protection law, individuals have a number of rights in relation to their personal data.

(a) The right to information: As a data controller, we must give you a certain amount of information about how we collect and process information about you. This information needs to be concise, transparent, understandable and accessible.

(b) The right of subject access: If you want a copy of the personal data, we hold about you, you have the right to make a subject access request (SAR) and get a copy of that information within 30 days.

(c) The right to rectification: You have the right to ask us, as data controller, to correct mistakes in the personal data we hold about you.

(d) The right to erasure (right to be forgotten): You can ask us to delete your personal data if it is no longer needed for its original purpose, or if you have given us permission to process it and you withdraw that permission (or where there is no other lawful basis for processing it).

(e) The right to restrict processing: In certain circumstances where, for lawful or legitimate purposes, we cannot delete your relevant personal information or if you do not want us to delete it, we can continue to store it for restricted purposes. This is an absolute right unless we have a lawful purpose to have it that overwrites your rights.

(f) The obligation to notify relevant third parties: If we have shared information with other people or organisations, and you then ask us to do either (c), (d) or (e) above, as data controller we must tell the other person or organisation (unless this is impossible or involves effort that is out of proportion to the matter).

(g) The right to data portability: This allows you to transfer your personal data from one data controller to another.

(h) The right to object: You have a right to object to us processing your personal data for certain reasons, as well as the right to object to processing carried out for profiling or direct marketing.

(i) The right to not be evaluated on the basis of automatic processing: You have the right not to be affected by decisions based only on automated processing which may significantly affect you.

(j) The right to bring class actions: You have the right to be collectively represented by not-for-profit organisations.

11. Subject access requests

You are entitled to ask us, in writing, for a copy of the personal data we hold about you. This is known as a subject access request (SAR). In line with legislation, we will not charge a fee for this information and will respond to your request within one month. This is unless this is not possible or deemed excessive, in which case we will contact you within the month of making the SAR.
Our members or anyone else we hold personal data about can also ask for information from local Scouting. The relevant Scout Group, as data controller in their own right, must answer these requests. Rosyth District Scouts is not legally responsible for these local SARs but we advise Scout Groups to respond to them in line with the law (that is, within the specified one-month time frame and without asking for a fee).

12. Further information and contacts

Requests for further information and Subject Access Requests for data held by Rosyth District should be made by email to Terry O'Neill, District Commissioner, rosythdc@yahoo.co.uk