South Leeds and Morley District Scout Council Data Protection Policy

Contents

Purpose of this policy and what it covers.

This policy sets out South Leeds and Morley Scout District's approach to protecting personal data and explains your rights in relation to how we may process personal data. We provide more detail in respect of how we process and protect your data below, particularly in section 5. This policy does not cover Individual groups as each as registered as an independent charity however it dies cover explorer units are they are district ran.

South Leeds and Morley Scout District ("We" in this document) is registered at the following address: 6 Woodkirk Gardens,DEWSBURY, WF12 7HZ. If you have any queries about anything set out in this policy or about your own rights, please write to the Data Protection Officer email at DPO@slamscouts.org.uk.

We may from time to time make minor changes to this policy. We will notify you directly when we make any substantial or significant changes to the policy.

Important definitions

'We' and 'The District' means South Leeds and Morley District Scout Council.

'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.

'Local Scouting' and 'Scout unit' mean Scout Groups within the South Leeds and Morley District.

'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 the deletion, rectification and restriction of processing.

‘Compass’ Compass is The Scouts Association’s membership system. Local Scouting must comply with the Data Protection Act 2018 and the GDPR when using Compass, The Scout Association’s Membership System.

‘OSM’ Online Scout Manager is the digital platform many groups and district sections use for storing and processing personal data.

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 can all be defined as personal data.

Some categories of personal data are recognised as being particularly sensitive (“special category 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.

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 units 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.

Each Scout unit will have its own data protection policy and it is expected to state that it adheres to this policy. In case of any doubt or questions you are advised to contact the Scout unit directly or to write to our Data Protection Officer at the above address who may be able to help.

What type of personal data do we collect and why?

Members and Volunteers

We benefit from the service of a large number of members giving their time to Scouting at both District and local Scouting levels. We hold personal data (including special category data) about adult members and volunteers on our membership database. We believe it is important to be open and transparent about how we will use your personal data. Information we hold about you may include 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
- details about your role(s) in Scouting
- details about your membership status
- race or ethnic background and native languages
- religion
- 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 also to help us if you leave or re-join).

Much of this information is collected from the member joining forms.

Young People

We may capture information on Young People who attend any events managed by The District, this may include details on dietary and accessibility requirements. We may also process data on Young People where they are part of a legal claim, the data we capture

may include the detail of the claim itself. This Data will be deleted as outlined in our data retention policy

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 about our work and campaigns and how they can support us further. This may include details of donors that wish to leave a legacy in their Will. We may hold the type of information as set out in Members and Volunteers

Customers and visitors

We also hold personal data from customers and visitors to our Badge Shop, and activity centres. We may hold the type of information as set out in Members and Volunteers also including the following:

- purchase history
- taxpayer and payment details
- Much of this information is taken from online registration forms.

Contractors (past, present and future)

As an employer, we need to keep information relating to each contractor who has a contract with us. This will include the pre-employment stage, references, and records relating to the time they worked.

We also hold information that allows us to pay Invoices. Information we may hold about Contractors includes the following:

- name and contact details
- length and periods of work to allow accurate payments
- details of training you receive
- details of your experience, qualifications, occupation, skills
- details of any health conditions

- details of disclosure checks if applicable
- information that allows us to pay Invoices
- references, and records relating to the time they worked for The District,
- Much of this information will be taken from the Invoice and other conversations in the contracting process.

Conditions for collecting personal data.

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:

Consent - you have to give (or have given) your permission for us to use your information for one or more specific purposes

Performance of a contract - we need to process the information to meet the terms of any contract you have entered into (for example when we process personal data as part of a volunteers membership application or to provide goods or services purchased with us)

Legal obligation - processing the information is necessary to keep to our legal obligations as data controller

Vital interests - processing the information is necessary to protect your vital interests

Public task - 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 examples)

Lawful basis	Data processing examples
Consent	• Sending marketing information not deemed part of legitimate interest • The use of photography captured by District • Managing grant applications and provisions • Accessing personal data on OSM. District will become an independent data controller of the youth member data that they access on OSM, as they will determine what they do with that data, for example adding the data to internal safeguarding

	case management systems. This will only happen after consent has been given by the Scout Group trustee board via OSM and the access will only ever include data that is necessary to fulfil this purpose
Performance of a contract	• Volunteers membership application • Supply of goods or services purchased
Legal obligation	• Responding to information requests from statutory authorities • Disclosure and Barring Service referral • Insurance underwriting referrals
Vital interests	• Medical history disclosure to a medical professional to protect the vital interests of the data subject
Public task	• The District use other more appropriate lawful basis for processing personal data
Legitimate interest	• Photography at District organised events where consent is not appropriate (could include the publishing of the photography in District media channels including printed format) • The passing of personal data to local Scout Groups as part of the 'Find a local group' service online. • Displaying the contact details of local leaders as part of the 'Find a local group' service online • Nominations for top awards • Informational/operational communications directly to volunteers • The use of membership data for the recruitment of District roles • The passing of volunteer and young person data to UKHQ in defence of cases

	• Scout Stories are submitted to Scouts HQ and may be published online

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

Information that we share

We may have to share your personal data within appropriate levels of the Association and with local Scouting, as long as this is necessary and directly related to your role within Scouting.

District may share personal data with its partners, companies and organisations and individuals who help us to fund, organise and operate events, projects, programmes and other activities. Our legal basis for doing this is to pursue our legitimate interest of being able to work collaboratively with other organisations to operate and administer the event, project, programme or activity.

Some of these organisations may process information in countries outside the EEA, such as the United States, where data protection laws are not the same as in the EEA. District will always ensure any transfer is subject to appropriate security measures to safeguard your personal data. Where transfers are necessary to countries where data protection has not yet been declared to be adequate, we rely on appropriate safeguards, as defined in the GDPR for these transfers. Full details of these organisations, confirmation of where they would process personal information, and details of the steps District have taken to safeguard personal data will be provided to data subjects at the time any personal data is collected.

We do not share personal data with companies, organisations and people outside the Association, unless one of the following applies;

- We have a clear lawful basis to do so.
- If we have to supply information to others (for example event providers) 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.

Keeping personal data secure

Everyone who handles personal data (including members and volunteers) must make sure it is held securely 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 taken off-site. The following is general guidance for everyone working within Scouting, including members and volunteers in local Scouting.

- You must only store personal data on networks, drives or files that are password protected and regularly backed up.
- You should keep paper records containing personal data secure. If you need to move paper records, you should do this strictly in line with data protection rules and procedures.
- You should not download personal data to mobile devices such as laptops and USB sticks unless necessary. Access to this information must be password protected and the information should be deleted immediately after use.
- You must keep all personal data secure when travelling.
- Personal data relating to members and volunteers should 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. Memory sticks should 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 data breach, you should follow your defined breach response process.
- All members undertake regular training to ensure that they are aware of the above rules.

Responsibilities

We expect our trustees, volunteers, members and any providers we use to keep to the guidelines as set out in our Data Policy and under ICO and GDPR guidance when they are using or processing personal data and other confidential or sensitive information. This is set out more clearly below.

Board of Trustees

Our Board of Trustees has overall responsibility for making sure that we keep to legal requirements, including data protection legislation.

Data protection officer (DPO) or equivalent role holder

District has appointed a DPO to ensure the organisation is monitoring compliance with GDPR and other Data Protection laws, our data protection policies, awareness- raising, training, and audits. Local Scouting Units should consider appointing their own DPO. 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.

Volunteers, members, and local Scouting

- We expect you to keep to data protection legislation and this data protection policy, and to follow the relevant rules set out in Headquarters Policy, Organisation and Rules (POR).
- The local Trustee board (trustees of local Groups, Districts, Areas, Counties, Countries and so on) 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 Trustee board) any instance where the rules on how we handle personal data are broken (or might be broken).

Data retention

We may keep information for different periods of time for different purposes as required by law or best practice. Individual departments include these time periods in their processes. We make sure we store this in line with our Data Retention Policy which can be found within the district policy SharePoint

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

Rights to accessing and updating personal data.

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

a) 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.

Subject access requests

You are entitled to ask us 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 calendar 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 to state the reason for the extension and/or the charging of an appropriate fee.

Our members or anyone else we hold personal data about can also ask for information from local Scouting. The relevant Scout unit, as data controller in their own right, must answer these requests. District is not legally responsible for these local SARs but we advise Scout units to respond to them in line with the law (that is, within the specified one calendar month time frame).

Further Information and contacts

Data protection officer contact details

dpo@slamscouts.org.uk

Subject access requests

Subject access requests for data held by The District should be made to our data protection officer at dpo@slamscouts.org.uk

Please note, subject access requests for data held by Local Scouting should be made directly to the relevant Scout unit as each Scout unit operates as a separate charity and each is a Data Controller in its own right.

In situations where you feel The District has not handled your personal data query/complaint appropriately you have the right to inform the Information Commissioners Office

Written on: 12th Mar 2023 Last updated: 8th Feb 2024 Published: 13th May 2024