Data Protection Policy

April 2024

Introduction

The Scout Association's commitment to protecting privacy and data forms a key policy for Scouting. This policy underpins both this Data Protection Policy and other associated policies used by The Scout Association, local Scouting and its membership. Each Local Scout Group, District and County are their own distinct data controllers, separate to The Scout Association (TSA) and separate legal entities. This means they are directly responsible for any personal data they process and must ensure that they are aware of their responsibilities under the law. We provide general guidance and signposting to local scouting, including online resources such as our Scout Unit Data Protection Toolkit.

Collapse all

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

This policy sets out The Scout Association'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. The Scout Association ("We" in this document) [is registered with the Information Commissioner's Office at] the following address: Gilwell Park, Chingford, London E4 7QW. If you have any queries about anything set out in this policy or about your own rights, please write to the Data Protection Officer (Black Penny Consulting) at the above address or via email at Enquiries.dpo@scouts.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.

2. Some Important Definitions

'We' means The Scout Association and The Scout Association Trust Corporation

'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, Districts, Counties, Areas (Wales), Regions (Scotland) or Countries. ‘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.

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 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.

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 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.

There are scenarios of joint controllership of personal data between The Scout Association and local Scouting, this is regarding the data held within Compass and specifically for the activities below:

- Maintenance of local Scouting's primary records, such as name, address and leadership details of the local Group, District, County, Area(Wales), Region (Scotland) or Country.
- Local Scouting roles, such as creation, management and deletion of role and any reasons for leaving local Scouting. This includes ID checking.
- Direct messaging in the platform.
- Training updates and Personal Learning Plan.

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 (Black Penny Consulting) at the above address who may be able to help.

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

We benefit from the service of a large number of members giving their time to Scouting at both UKHQ 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.

5.2 Young People

We do not centrally hold a youth membership database. The responsibility for managing youth membership sits locally. However, we do process some personal data about young people.

For Young People, we may hold information where there has been a safeguarding case raised, this may include basic personal identifiers along with the details of the case. We may capture information on Young People who attend any events managed by The Scout Association, this may include details on dietary and accessibility requirements. We may process data about young people where they have been put forward for an award, entered a competition run by TSA or partaken in research undertaken by TSA. 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.

5.3 Trustees and members of the governance structure

For the members of The Scout Association's Board of Trustees and its subcommittees, other committees and working groups, we may hold the type of information as set out in 5.1 and also including the following:

- CVs,
- Related party information.

5.4 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 following type of information:

- name and contact details,
- address,
- details of donations and interactions, such as communications and events.

Where TSA has assessed you as a major donor (based on donations of £10,000 and above), we may hold publicly available details that assist us in assessing your:

- capacity to give,
- propensity to give,
- closeness to the Scouts.

5.5 Customers and visitors

We also hold personal data for visitors to our sites. This can include guests, suppliers, tradespeople and contractors. We may hold the type of information as set out in 5.1. Much of this information is taken from online registration forms and sign-in mechanisms.

5.6 Employees and contractors (past, present and future)

As an employer, we need to keep information relating to each member of staff and contractors who has a contract with us. This will include the pre-employment stage, references, and records relating to the time they worked for us including probationary, appraisal and disciplinary information.

We also hold information that allows us to pay salaries and work with other payroll and pension providers. Information we may hold about staff 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.
- details of next of kin.
- age/date of birth.
- details of any health conditions.
- details of disclosure checks if applicable.
- details of any dependents.
- information that allows us to pay salaries and work with other payroll and pension providers.
- references, and records relating to the time they worked for TSA.
- probationary, appraisal and disciplinary information.

Much of this information will be taken from the job application form.

We have a separate Staff Privacy Notice which provides more detail to staff members about how we process their data.

5.7 CCTV

Our UK Headquarters operates a CCTV network to help prevent and detect crime and safeguard (protect) young people and others. If we can identify somebody from a CCTV image, the image must be processed as personal data. This is supported by a CCTV Policy.

5.8 Scout Association Trust Corporation (SATC)

The Scout Association Trust Corporation (SATC) hold title to property on behalf of Scout units. As part of the service that SATC provides, we are required to receive and post hard copy documents and in many instances, require some personal information in order to provide this service. Invariably the information that we may require is limited to name and contact details including postal address.

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:

- **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 volunteer's 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 UKHQ. • Managing TSA HQ grant applications and provisions. • Accessing personal data on OSM. TSA 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 Executive Committee 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	• Sharing information with statutory bodies such as the Police (including the Hydrant Programme) or Local Authorities.
Legitimate interest	• Photography at UKHQ organised events where consent is not appropriate (could include the publishing of the photography in TSA 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 Meritorious Conduct & Gallantry Awards, The Cornwell scout badge, Chief Scout's Personal Awards and Good Service Awards. • Informational/operational communications directly to volunteers. • The use of membership data for the recruitment of HQ roles. • The passing of volunteer and young person data to TSA's outside legal counsel 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.

6.2 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.

TSA 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 UK/EEA, such as the United States, where data protection laws are not the same as in the UK/EEA. TSA 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 UK GDPR for these transfers. Full details of these organisations, confirmation of where they would process personal information, and details of the steps TSA have taken to safeguard personal data will be provided to data subjects at the time any personal data is collected.

TSA may also share your information within the TSA group of companies, for the purposes of managing the particular events, projects, programmes, or other activities. TSA currently provides all support and services for its subsidiary companies, therefore, our legal basis for sharing information is to pursue the legitimate interests of shared resources and management reporting between the companies within the group.

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 payroll 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.

View a list of the most common third parties we share personal data with. This is not exhaustive and acts as an example, however TSA ensures that where data processing may include a third party, the data subject is informed, this is usually at the point data is captured.

7. Keeping personal data secure

Everyone who handles personal data (including staff, members, volunteers, payroll and pension providers) 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 staff aware of these steps, including keeping to our internal information and computing technology (ICT) policy. 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 staff, 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 have proper entry-control systems in place, and you should report any stranger seen in entry-controlled areas.
- 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 staff undertake regular training to ensure that they are aware of the above rules, and work to an agreed Acceptable Usage Policy when using IT equipment.

8. Responsibilities

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

8.1 Board of Trustees

Our Board of Trustees has overall responsibility for the Association and for making sure that we keep to legal requirements, including data protection legislation. Our CEO and senior leadership team are responsible for making sure we keep to these requirements across UKHQ.

8.2 Data protection officer (DPO) or equivalent role holder

TSA has externally 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.

8.3 Staff

All staff have a responsibility to keep to the requirements of this data protection policy and our related procedures and processes. Managers are responsible for

making sure that staff within their teams are aware of and keep to this. If you become aware of a data protection issue you must report it promptly to the data protection officer or equivalent role holder.

If you do not adhere to this data protection policy and its associated policies and procedures, we may take disciplinary action against you.

8.4 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 our Policy, Organisation and Rules (POR).

The local Executive Committee (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, Data Leads, 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 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.

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 staff 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 calendar month, though if the request is deemed to be complex we may take up to three months. If the request is deemed excessive, we will contact you within the month of making the SAR to state the reason and discuss how we will proceed which may include making a charge.

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. UKHQ 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).

12. Further information and contacts
Data protection officer contact details: Enquiries.dpo@scouts.org.uk

Subject access requests

Subject access requests for data held by The Scout Association UKHQ should be made to our UKHQ legal department at DSARS@scouts.org.uk or by writing to:

The Scout Association
Legal Services
Gilwell Park
Chingford
London
E4 7QW.

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.

Queries or concerns about how personal data is managed at TSA should be directed to Enquiries.DPO@scouts.org.uk. The Information Governance Team will respond to you within one month, or where an issue is deemed complex, no later than three months.

In situations where you feel The Scout Association has not handled your personal data query/complaint appropriately you have the right to inform the Information Commissioners Office, though you may contact them at any time.

Contact the Information Commissioner's Office.