Scouts
Grafton

General Data Protection Regulations (GDPR) Policy

Last Updated: October 2025

Scouts
Grafton

Introduction

Privacy and data protection is a key policy for Scouting and the Association is committed to protecting privacy and data protection.

This policy sets out Grafton District Scout's (GDS) commitment to data protection, and the rights and obligations of Adult Leaders, Young People, the District Scout Council and others involved with GDS (individuals) in relation to personal data and its compliance with the General Data Protection Regulations 2018 (GDPR).

GDS is committed to being transparent about how it collects and uses the personal data of individuals and to meeting its data protection obligations. This policy also complies with the Scout Association's Data Protection Policy.

This policy applies to the personal data of applicants, current and former members, referred to as "people related personal data".

Definitions

Personal data is information relating to natural persons who can be identified or who are identifiable directing from the information in question, or who can be indirectly identified from that information in conjunction with other information.

Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

Special categories of personal data mean information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

Criminal records data e.g. a DBS means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

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.

What type of personal data do we collect and why?

Members & Volunteers

We may hold personal data (including special category data) about members (including young people) and volunteers on our membership databases. 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
- Nationality
- Bank account details
- Gift Aid eligibility

We need this information to communicate with you, set you up with access to any systems we use, understand your physical and mental wellbeing and to carry out any necessary checks to make sure that volunteers 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 and stored in the national membership database or “Online Scout Manager”. We may also process sections of this data using our corporate GDS Google Workspace tenancy.

Trustees and members of the governance structure

For the members of GDS’s Board of Trustees and any subcommittees, other committees and working groups, we may hold the type of information as set out above and also including the following:

- CV's
- Related party information or conflicts of interest

Donors

We benefit from donations from members of the public and other charitable organisations / businesses who support our work, and we hold personal data about these donors so that we can process donations, collect gift aid and tell donors about our work and campaigns and how they can support us further. We may hold the type of information as set out in "Members & Volunteers".

Customers and visitors

We also hold personal data from customers and visitors to our Badge Shop, Bookings Site and Spotley Wood Campsite. We may hold the type of information as set out in "Members & Volunteers" and also including the following:

- Purchase history
- Taxpayer and payment details

Much of this information is collected via online registration forms.

Data Protection Principles

GDS processes people related personal data in accordance with the following data protection principles:

- Processes personal data lawfully, fairly and in a transparent manner
- Collects personal data only for specified, explicit and legitimate purposes
- Processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing
- Keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay
- Keeps personal data only for the period necessary for processing
- Adopts appropriate measures to make sure that personal data is secure, protected against unauthorised or unlawful processing, accidental loss and destruction or damage
- GDS tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its Privacy Notice. It will not process personal data of members for other reasons
- GDS will only process special categories of personal data or criminal records data to perform obligations or to meet the obligations of Scout activities in accordance with the requirements of the GDPR. GDS will request explicit consent from the individuals prior to processing sensitive data, for example gathering health related data prior to a camp.
- GDS will update people related personal data promptly if an individual advises that their information has changed or is inaccurate.
- Personal data gathered during the relationship with GDS will be held in a variety of locations, in hard copy, electronic format or both and on GDS systems. The periods for which the GDS holds people related personal data are available in the Data Retention Policy.

Individual's Rights

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

- 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.
- 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.
- 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.
- 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).
- 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.
- 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).
- The right to data portability: this allows you to transfer your personal data from one data controller to another.
- 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. GDS can refuse to comply with an objection if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.
- 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.
- 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, 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.

- GDS will provide the Individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the Individual has made a request electronically, unless they agree otherwise.
- To make a subject access request, the Individual should send the request to the District Lead Volunteer in writing. In some cases, GDS may need to ask for proof of identification before the request can be processed.
- GDS will inform the individual if it needs to verify their identity and the documents it requires.
- GDS will normally respond to a request within a period of one month from the date it is received. In some cases, such as where GDS processes large amounts of the Individual's data, it may respond within three months of the date the request is received. GDS will write to the Individual within one month of receiving the original request to tell them if this is the case.
- If a subject access request is manifestly unfounded or excessive, GDS is not obliged to comply with it.
- A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which GDS has already responded. If an Individual submits a request that is unfounded or excessive, GDS will notify them this is the case and whether or not it will respond to it.

Other Rights

Individuals have a number of other rights in relation to their personal data. They can require GDS to rectify inaccurate data and stop processing or erase data:

- That is no longer necessary for the purposes of processing
- If the individual's interests override GDS's legitimate grounds for processing data (where GDS relies on its legitimate interests as a reason for processing data)
- If processing is unlawful; and
- For a period of time if data is inaccurate or if there is a dispute about whether or not the individual's interests override GDS's legitimate grounds for processing data.

To ask GDS to take any of these steps, the individual should make a request in writing to the District Lead Volunteer.

Data Security

GDS takes the security of personal data seriously. Everyone who handles personal data on behalf of GDS 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 volunteers aware of these steps. In most cases, personal data must be stored in appropriate systems and encrypted when being transported. The following is general guidance for everyone working within GDS.

- It is expected that individuals will store data within GDS systems which are password protected and regularly backed up. Should individuals require data to be stored outside of these systems, they must only store personal data on appropriate media devices or systems that meet the necessary security standards, including, but not limited to, encryption and access control. Approval should be sought from the District Lead Volunteer before using any non GDS system.
- You should not download personal data to personal devices such as laptops and portable media devices unless absolutely necessary. Access to this information must be password protected, and the information should be deleted immediately after use. Contact information should only be stored on the national membership system, OSM or the GDS Google Workspace tenant.
- You should keep paper records containing personal data secure e.g. in a locked filing cabinet. If you need to move paper records, you should do this strictly in line with data protection rules and procedures.
- You must keep all personal data secure when travelling e.g. lockable briefcase, lock box or secured dry bag in a zipped pocket on your person.
- Personal data relating to members and volunteers should usually only be stored on the appropriate membership database (national membership system for Adults or Online Scout Manager for young people) which are known to have the appropriate security in place. Data may also be processed or stored on the GDS Google Workspace system.
- Any paper forms used to collect personal data should kept to a minimum and securely destroyed once they are no longer required. Paper forms should be used to collect data only.

- When sending larger amounts of personal data by post, you should use registered mail or a courier. Memory sticks must be encrypted.
- All GDS appointments are required to use approved systems sanctioned by the District Leadership Team including the District's Google Workspace system for all Scouting related email communication. Google Chat is the preferred platform for other comms and transmission of personal or sensitive data as they offer encryption.
- When sending personal data by email, this must be appropriately authenticated, and password protected. It is preferable to share private authenticated links to documents within the GDS Google Drive system rather sending attachments via email.
- Do not send financial or sensitive information by email unless it is has additional layers of security such as password protection or secondary encryption.
- You should not share your passwords or additional security factors 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 should inform the District Lead Volunteer immediately

Data Breaches

If GDS discovers that there has been a breach of people related personal data that poses a risk to the rights and freedoms of members, volunteers or customers, it will report it to the Information Commissioner within 72 hours of discovery

International Data Transfers

People related personal data may be transferred to countries outside the EEA. Data can only be transferred for legitimate Scouting reasons e.g. organising a visit to another country.

Volunteers in GDS are responsible for screening personal data and requesting Individual explicit consent prior to any international data transfer.

Individual’s Responsibilities

Individuals are responsible for helping GDS to keep their personal data up to date. Individuals should let GDS know if data provided to GDS changes, for example if an Individual moves to a new house or changes their bank details.

Individuals may have access to personal data of other Individuals in the course of undertaking their Scouting role. Where this is the case, GDS relies on Individuals to help meet its data protection obligations to all Individuals.

Individuals who have access to personal data are required:

- To access only data that they have authority to access and only for authorised purposes;
- Not to disclose data except to Individuals or others who have a legitimate need to know;
- To keep data secure, for example taking adequate precautions to prevent unauthorised access to premises, computer access, including password protection and secure physical file storage and destruction;
- Not to remove personal data, or devices containing or that can be used to access personal data, without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device and;
- Not to store personal data on local drives or on personal devices that are used for Scouting purposes. All data must be stored on either the national membership database, Online Scout Manager or the GDS Google Workspace system. Individuals should not send personal information using personal email accounts.
- To destroy or return any personal holdings of such data when there is no further need for it.

Failing to observe these requirements may amount to a disciplinary or dismissal, which will be dealt with under the Scout Association’s appointments process. Significant or deliberate breaches of this policy, such as accessing Individual’s data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to membership of the organisation being ended immediately and/or legal action.

Training

GDS will provide training to all Individuals about their data protection responsibilities as part of the induction process. As required in POR, all roles are required to complete mandatory GDPR learning within 6 months of appointment.

Policy Ownership

This policy is owned by the District Leadership Team and may be amended at any time.

Further information

For further information, please contact the District Lead Volunteer on dlv@gdscouts.org.uk.

Subject Access Requests
Subject Access Requests for data held by GDS should be made to the District Lead Volunteer on dlv@gdscouts.org.uk or by writing to:

Grafton District Scouts
c/o 35 Centurion Way
Wootton
Northampton
NN4 6LD

Please note that Subject Access Requests for data held by Groups should be made directly to the relevant Group Lead Volunteer or Group Trustee Board as each Scout Group operates as a separate charity and are therefore each a Data Controller in their own right.

Document Change Log

Version	Date	Change	Author
1	May 2025	Creation of Policy	WHa
1.1	October 2025	Minor Re-words	GSi