



Bramley Scout Group
Data Protection Policy and Procedures
Approved 08 May 2025

Bramley Scout Group

Data Protection Policy and Procedures

Contents

BSG Adult Volunteer Responsibilities	3
Collection, Storage and Retention of Data	3
How we collect and store data and who we share it with.	4
How do we look after/handle the data?.....	4
How long do we keep data?	5
How do we destroy data?	5
Privacy statements	5
Security of Data	5
Introduction of Microsoft Forms	5
Online Scout Manager (OSM)	5
Communication by E-mails	5
Recording Accidents.....	6
Keeping data safe during 'Events and Trips'.....	6
SharePoint	6
Personal Computers.....	6
Photographs and videos.....	6
Social media.....	7
Digital Password Convention.....	7
What are individuals entitled to know about the data we hold about them?.....	7
How are we providing this information?	7
Dealing with Data Requests.....	8
Responding to Data Breaches	8
Third parties.....	8
Compliance and Disciplinary Procedures.....	8
Appendix 1: Definitions and Abbreviations.....	9
Appendix 2: Data Protection Principles	9
Appendix 3: GDPR Documents maintained by the Group.....	10

Introduction

This document is Bramley Scout Group's Data Protection Policy and Procedures for its Adult Volunteers. This document provides information for Adult Volunteers to ensure their understanding and compliance with the Data Protection Act 2018 and General Data Protection Regulations (GDPR).

As a Group, we have to ensure that data is adequately protected and maintained and to ensure that when it is no longer needed or of no value it is discarded at the appropriate time.

The Bramley Scout Group has separate Privacy and Data Retention Policies which are for public information and are displayed on our website and must be notified to individuals at the time of data collection (e.g. when collecting data for waiting list and with new joiner's forms).

BSG Adult Volunteer Responsibilities

As an Adult Volunteer you are responsible for ensuring that:

- you are familiar with, and follow, this Data Protection Policy (in particular the procedures included in the Security of Data section below)
- any personal data that you hold, whether in electronic or paper format, is kept securely;
- personal information is not disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;
- Data is not divulged outside of the Group except where required for legal reasons, for example Safeguarding;
- any information you have provided in connection with your role is accurate and up-to-date;
- the Group is notified of any changes to this information, e.g. changes of address

For the avoidance of doubt – Personal data means any data held which can be identified as belonging to an individual person.

Collection, Storage and Retention of Data

What data we collect and why we need it.

We have completed a Data Inventory to assess the data we collect as a Group. This will be reviewed on an annual basis to ensure that it is up-to-date and accurate and that this policy reflects all the data we collect. We have also assessed whether this data is collected for legitimate interests and ensured that we do not collect any personal data we do not need.

We collect information such as:

- Contact details for our Adult Volunteers, Young Persons and their Parents/(Guardians) so that we can contact them regarding our activities and also contact the relevant people in the event of an emergency;
- Health and medical information for our Adult Volunteers and Young Persons so that we are aware of any medical history and so we can ensure that the person is fit and able to take part in a particular activity or so that we can administer required medications;
- Details of any disabilities so that we can adapt our programme accordingly;
- Criminal record checks for volunteers (these are required for recruitment but are not stored);
- Data required for the purposes of reclaiming Gift Aid (name and address of donor);
- Data required to maintain the Waiting List (name, address, date of birth and parents' contact details);
- Accident and incident reporting forms which will contain details of the people involved;
- Photographs and videos are sometimes taken during activities and events.

How we collect and store data and who we share it with.

Type of Data	How it is collected and stored	Who has access to it
Waiting List	District web forms and/or email which is then entered into OSM and Microsoft Excel	Waiting List Administrator and certain individuals at District level. Shared with appropriate Team Leader when space becomes available.
Young Person joining information	Microsoft Forms held on Sharepoint which is then entered into OSM.	Waiting List Administrator, the Team Lead Volunteer, Team Leaders and Team Members, the Treasurer and certain individuals at District level. *
Additional Information required for Activities or Events	Microsoft Forms or email	Adult volunteers or external providers who are attending or running the activity or event.
Adult Volunteer information	District Adult Volunteer webform which is then input into The Scout Association Digital System and OSM.	Team Lead Volunteer and certain individuals at District level have access to both systems. Team Leaders and Team members have access to the data in OSM.
Gift Aid declarations	Microsoft Word or Adobe Acrobat form. If returned as a paper form this will be scanned and held as a PDF file and the paper form destroyed.	Treasurer
Statistical data regarding our Young Persons and Adult Volunteers	Collated on OSM	Team Lead Volunteers shares the data with The Scout Association

*Access to OSM by leaders is generally restricted to the leader's own section, but can be extended to other sections where there is an administrative need. When a Young Person moves from one section to the next we will pass the information we hold onto the new Team Leader using OSM. If the Young Person is moving outside of BSG e.g. to another Group or to Explorers, then the Team Leader or Treasurer must obtain permission from the parent/guardian prior to transfer.

We may also share data with other offices where we are required to do so by law, or for example for the protection of the Young Person whilst in the care of the Group.

We do not use any data for the purposes of marketing, other than photographs which may be included in local magazine articles or on recruitment posters. Consent for use of photographs must be obtained.

How do we look after/handle the data?

Adult Volunteers are given a copy of this Policy and informed of the data protection principles (see Appendix 1).

To ensure we achieve these principles, we will:

- Ensure the protection of all data.
- Only permit individuals to access and view data which is necessary for the performance of their role and to safeguard Young Persons in our care, and ensure those individuals are aware of their responsibility to ensure the data is used for the purpose it is meant.
- We will ensure that all Adult Volunteers understand and comply with the Data Protection Policy and be aware of their responsibility to report any vulnerabilities or issues.
- Ensure Adult Volunteers are aware that they must protect Bramley Scout Group ("BSG") from liability or damage through unauthorised actions.

How long do we keep data?

Data is retained in accordance with our Data Retention Policy.

Individuals responsible for the retention of data are also responsible for the destruction of data following the retention period.

How do we destroy data?

Data is destroyed in such a way as to ensure that all sensitive or confidential material can no longer be read or identified to a particular individual.

Privacy statements

When requesting personal data from members or their parents, we should include a privacy statement. A template is available for this purpose. It should be added to all documents and emails requesting personal data.

Security of Data

All Adult Volunteers should adhere to the following security procedures.

Introduction of Microsoft Forms

To collect data securely, please use Microsoft forms wherever possible. This will ensure data is collected in a secure, organised in a format which is the same throughout the process, and allow us to be more sustainable to environment. For more information – and an easy guide for how this works, please visit the website below.

[Introduction to Microsoft Forms - Microsoft Support](#)

Online Scout Manager (OSM)

- Access to OSM should only be granted to Adult Volunteers who have completed the DBS check.
- Access should only be given to the data on OSM which they require to fulfil their role within the Group.
- Access should be revoked as soon as the Adult Volunteer leaves the Group.
- Young Persons should be removed from OSM or transferred to another Group or Section within 1 month of them leaving the Group/Section. (The existing leader must confirm that the information is up-to-date prior to transfer.)
- If the Young Person is moving outside of BSG e.g. to another Group or to Explorers, then the Section Leader or Group Administrator must obtain permission from the parent/guardian prior to transfer.
- Parents should be asked to confirm once a year that the data held on OSM in respect of their child is up-to-date and accurate.

Communication by E-mails

- All Adult Volunteers will be provided with a @bramley-scout email address. This should be used for all emails relating to Scouting. Personal email accounts should not be used for scouting emails. This ensures that Adult Volunteers have access to the correct addresses for all other Adult Volunteers through the use of Distributions Lists and also means that all Scouting emails are accessible in a Scouting inbox which will be required in the event of a Data Access Request. This means that the Volunteer will lose access to the account when they leave the Group and hence not have access to any personal data contained within those emails.
- Consent to use a parents' email address and to send internal emails regarding the Young Person will be obtained from all parents when the Young Person joins the Group.
- Emails regarding a particular Young Person should only be sent to that person's parent or guardian or to other Adult Volunteers within the Group if they require that information in order to fulfil their role within the Group.

- Where it is necessary to email data regarding the whole Group or a Section within the Group, for example where you are sending a list of contact details for an organised activity to the Emergency Contact person, this should be sent in an attachment which is protected by a password which must follow the password convention below.
- Take care when using Reply to All, as you may not want all e-mail participants to be part of any on-going communication.
- Always delete emails when they are no longer required especially where they contain data attachments – check Inbox folder, Sent Items folder and Deleted folder;
- Don't forget to empty your Deleted Items folder;
- If you are sending an Email to multiple individuals ALWAYS use the "BCC" field – remember that E-mail addresses are also personal data. NB OSM sends emails on a BCC basis.
- Remember that a data subject can request a copy of all data we hold with respect to them, this would include copies of all emails, so bear this in mind when writing emails and only include wording that you would be happy to share with that individual!

Recording Accidents

All accidents should be recorded using the Accident forms in OSM. Paper accident books should no longer be used as these are less secure.

Keeping data safe during 'Events and Trips'

You will have electronic copies of all personal data for trips and events. However, there are times where it is necessary to carry paper copies, as sometimes connection issues may occur. Therefore, when going on such outings, please take paper copies of medical records, emergency contact details and list of attendees with you. These should be kept securely with the leaders, in a secure environment that ensures they are safe, and unable to be damaged. Once the event is over, please ensure all details are shredded and destroyed confidentially.

SharePoint

SharePoint is a secure Microsoft system that should be used to save all scouting documents.

Personal Computers

When using a personal computer or tablet to store or process data, it is essential to ensure the device is secure to protect sensitive information. This includes using strong passwords or biometric authentication, keeping operating systems and software up-to-date with the latest security patches, and installing reliable antivirus and firewall protection. Data should be encrypted where possible, and access to the device should be restricted to authorised users only. Regular backups should be maintained, and care should be taken not to store sensitive data in unsecured locations. Avoid using public Wi-Fi networks without a secure VPN to prevent unauthorized access. Data should be move to SharePoint whenever possible.

Photographs and videos

- Consent to take photos or videos of children is obtained when the Young Person joins the Group and is updated on OSM.
- All Adult Volunteers who take photos or videos of members of the Group should ensure that they know who we have consent to take photos of and they should endeavour not take photos of anyone for whom we do not hold consent for. This can be done in such a way so has not to draw attention to the Young Person – for example by positioning them at the end of the Group and cropping that Young Person out when taking the photograph.
- Where it may not be possible to have gained formal consent from every individual who may feature in photos or videos (for example of large events), then leaders should inform the parents and participants of their intention to take photos so that they can express their wishes.
- Where photos (or other digital assets) will be used for very public purposes, such as specific marketing (recruitment posters) or an editorial in the local magazine for example, Leaders or other Adult Volunteers should obtain specific consent from the parents for the photos to be used in that way. A Digital Asset Consent Form is available for this purpose. A written log of their name, date and what the consent was

for should be maintained, with evidence of consent if this is practicable (or a note that the consent was given verbally).

- Where photos are being used in an editorial, consider whether or not it is appropriate to use the Young Person's full name and age. Never use the full address of the person. A collective name eg Bramley Cubs may be more appropriate.
- We should also obtain the Young Person's permission to use their image. This does not need to be formal, but they should be made aware that you are taking photos and how they will be used.
- Photography, videos and audio of no use should be removed at source or in any copies when not needed.
- When using cloud services to store photos ensure that you use a reputable provider with guaranteed storage in the UK or EEA

Social media

- We have a separate Facebook Policy and Guidelines for Social Media Use which should be read and followed by all Adult Volunteers.
- WhatsApp Communities should be used instead of WhatsApp Groups as the former does not share telephone numbers with other members of the Community.

Digital Password Convention

Documents with personal and sensitive information which are being shared via email should be password protected. The password should be shared with the recipient by a different means to the way the document is shared eg by text message or WhatsApp.

Passwords:

- Must consist of at least 11 characters; and
- Must be a combination of letters, numbers and symbols; and
- Letters must be in a combination of upper and lower case;
- Must not contain whole words that are unique to you.
- Do not reuse passwords from other accounts

What are individuals entitled to know about the data we hold about them?

Individuals are entitled to know:

- what personal information the Group holds about them and the purpose for which it is used
- how to gain access to it
- how it is kept up to date
- what the Group is doing to comply with its obligations under the GDPR

How are we providing this information?

We publish our Privacy Policy and Data Retention Policy on our website which gives this information. Existing members, adult volunteers and new joiners and will be directed to the website. A Privacy Statement should be included on all forms and emails where personal data is requested.

Dealing with Data Requests

Individuals have rights in relation to information requests and rights to have their data removed from systems and paper files or rectified. They also have the right to request that we restrict further use of their data if they believe we are not processing it in accordance with our Privacy notice. They can also request that we export their personal data in a way that can be read digitally eg PDF.

A subject access request form is available on our website for individuals to make any of the above requests.

Any such requests must be referred to the Data Lead (as indicated on the form), nobody should action any such requests themselves. The Data Lead will review any such requests in conjunction with the provisions of the GDPR and Scout HQ guidelines and process accordingly, in addition a log will be kept using the Subject Rights Request Register. The Data Lead should respond to the subject access request within 30 days.

A Data Inventory is maintained in order to assist with subject access requests. This should be reviewed annually.

Responding to Data Breaches

There may be a rare occasion where a Data Protection breach occurs. Under the GDPR it is mandatory for any breach to be reported to ICO, however minor. The procedure for reporting breaches is as follows:

Adult Volunteers should report any Data Protection breaches immediately, however small, to the Trustee Board. This can be done using the Data Breach Notification Form. A Data Breach Register should be maintained of any breaches.

Following the reporting of the breach it is the responsibility of the Trustee Board to determine within 72 hours whether it should be reported to the ICO. They should also send a copy of the Data Breach Notification Form to The Scout Association.

Following the necessary actions, the Trustee Board will assess the incident overall and put measures or controls in place where applicable to ensure the incident does not happen again

It is implied that ICO will look more favourably to breaches that have been reported to them directly and will take a dim view on undisclosed breaches.

Third parties

We maintain a Third Party Register to capture any third parties that we use to process data. GDPR alignment statements should be obtained from any third parties who we are sharing data with to ensure that they comply with GDPR. This includes any third parties who organise events for the Group who require us to share details about the individuals taking part in the event.

Compliance and Disciplinary Procedures

All current Adult Volunteers will be notified of the existence of this policy and any breach will be dealt by the Trustee Board. All Adult Volunteers must also complete the GDPR training provided by the Scout Association within 5 months of joining the Group.

Any breach of the General Data Protection Regulations, either through negligence or deliberate act, may lead to disciplinary action being taken and could result in a criminal prosecution to either BSG and/or the responsible individual.

Appendix 1: Definitions and Abbreviations

Definitions

Data: For the purpose of this policy, “data” shall be interpreted to mean: any electronic record, papers, files, books, photographs, tapes, films, recordings, or other documentary materials, or any copies thereof, regardless of physical form or characteristics made, produced, executed, or received by any Adult Volunteer in connection with the operation of Bramley Scout Group (“BSG”).

Electronic record: The term “electronic record” means any record that is created, received, maintained or stored on local workstations or central servers.

Data Breach: The GDPR defines a personal data breach as “*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data*”. The Guidelines add that this includes even an incident that results in personal data being only temporarily lost or unavailable.

- **Confidentiality** – an unauthorised or accidental disclosure of, or access to, personal data, for example by sending an email to the wrong address, allowing an unauthorised person to view personal data.
- **Integrity** – an unauthorised or accidental alteration of personal data.
- **Availability** – unauthorised or accidental loss of access to, or destruction of, personal data e.g. deletion of data accidentally or by an unauthorised person, a lost decryption key in the case of encrypted data, or unavailability due to a power failure or service attack. It is important to note that an availability breach may occur even if data is only temporarily lost or unavailable, *although such a breach may not need to be notified unless it is likely to result in a risk to the rights of individuals in the given circumstances.*

Abbreviations

BSG – Bramley Scout Group

OSM – Online Scout Manager

District – Basingstoke East District Scout Council

Appendix 2: Data Protection Principles

Data must be:

- Processed lawfully, fairly and in a transparent manner;
- Obtained for specified, explicit and legitimate purposes and not processed in any manner incompatible with that purpose;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and where necessary kept up to date. Inaccurate data must be rectified or erased without delay;
- Kept for no longer than necessary for the purpose;
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures;

Appendix 3: GDPR Documents maintained by the Group

The following documents need to be maintained and regularly reviewed to ensure that they are up-to-date:

Document	Frequency of review	Last reviewed
GDPR Data Protection Policy and Procedures	Annually	May 2024
BSG Privacy Policy	Annually	May 2024
BSG Data Retention Policy	Annually	May 2024
GDPR Data Inventory	Annually	May 2024
GDPR Data Security Register	Annually	May 2024
GDPR Legitimate Interest Assessments	Annually	May 2024
GDPR Risk Register	Annually	May 2024
GDPR Third Party Register	Annually	May 2024
GDPR Privacy Statement template	Annually	May 2024

The following additional documents need to be maintained by the Board of Trustees:

Document
GDPR Data Breach Notification Form
GDPR Data Breach Register
GDPR Subject Rights Request Register

The following documents need to be made available to all members of the Group on our website:

Document
BSG Data Privacy Policy
BSG Data Retention Policy
Subject Access Request Form

The following templates are available:

Template
BSG Privacy Statement Template
BSG Digital Asset Consent Form

The following documents need to contain a Privacy Statement:

Document
Personal Information Forms – for Young Persons and Adult volunteers
Emails to people wanting to join the waiting list
Any requests for additional information for events