Scouts

Stockton, Thornaby & District

GDPR Compliance

v1.3 July 2020

Executive Summary

This document has been prepared by Shaun Jones, District Commissioner, on behalf of the District Executive Committee and aims to document the District's data collection and processing activities and our compliance with the GDPR.

We consider the data we collect and process, the reasons for this collection and processing. We examine where this data is held, how it is kept secure, where the data came from and on what lawful basis we process it. In addition to this we provide details of our retention policies, our data breach response plan and how we handle subject access requests.

Much of the information in this document is based on information from the Information Commissioners Office (ICO) and guidance from The Scout Association in the form of the GDPR toolkit which was produced in partnership with Black Penny Consulting.

Approved by the trustees on 17th September 2018, last reviewed 13th December 2019.

Contents

Organisational Details

Organisation name and contact details

Stockton, Thornaby & District Scout Council
26 Briardene Court
Bishopsgarth
Stockton-on-Tees
TS19 8UX

e: dc@stocktonthornabydistrictscouts.com
t: 07562 262449

Person/s responsible for data protection

The charity trustees, otherwise referred to as the District Executive Committee.

Purposes of Data Processing

The District collects and processes a variety of personal data for the purposes of facilitating a person's membership in Scouting or for providing services to another person or organisation. A short description of the reasons for processing this data is given under the headings of young people, adults and others below as the nature of this differs for each. Data flow maps for young person and adult membership processes are given in Appendix 1.

Young People

We have two categories of young people that we collect and process data about, young people who are making want to join enquiries and/or already in a Scout Group and Explorer Scouts and Young Leaders. The nature of the data we collect and process and the reasons for it differ therefore they are considered separately below:

a) Young people wanting to join and/or already in a Scout Group

The District collects data about young people from their parents when they make an initial 'want to join' enquiry. This data is used to place the young person on the relevant waiting list before allocating them in a place in a Scout Group.

Once a young person is a member of a Group the District processes data annually as part of the national Scout census this is to provide statistical information on the reach of Scouting across the UK and helps to facilitate appropriate insurance and resources.

From time to time the District will also collect and process data about young people already in groups in order to facilitate trips and other District led events.

As all safeguarding incidents within the District must be reported to the District Commissioner for referral to the Scout Association safeguarding team

by definition the District collects data relating to safeguarding incidents involving young people. This data is collected to ensure that the incident is recorded and dealt with by the necessary external agencies.

Generally the records made if a young person suffers an accident or injury are made and held by the group that they are a member of however from time to time during District led activities these records will be made and stored centrally.

b) Explorer Scouts and Young Leaders

The District collects data about Explorer Scouts and Young Leaders from their parents when they join. This data is used to facilitate their membership of an Explorer Scout unit or the Young Leaders unit.

Once a young person is a member of a unit the District processes data annually as part of the national Scout census this is to provide statistical information on the reach of Scouting across the UK and helps to facilitate appropriate insurance and resources.

In addition to this the District occasionally collects additional data in order to facilitate camps, trips and other activities.

As all safeguarding incidents within the District must be reported to the District Commissioner for referral to the Scout Association safeguarding team by definition the District collects data relating to safeguarding incidents involving Explorer Scouts and Young Leaders. This data is collected to ensure that the incident is recorded and dealt with by the necessary external agencies.

If an Explorer Scout or Young Leader suffers an accident or injury whilst on a District organised activity (or on a normal meeting night in the case of Explorer Scouts) data is recorded about the incident and the person or people involved. Accidents and or injuries involving Young Leaders during a section meeting at the group in which they are placed will be recorded by the group involved and subject to their own data protection policies.

Adults

The District processes data in relation to adults for two possible reasons:

a) To facilitate their membership of Scouting

The District collects and processes data about an individual when they submit such data via a 'want to join' enquiry. This data is processed to allow the adult to join Scouting and complete a DBS check as part of our safeguarding procedures.

The District collects and processes data relating to an adult volunteer's progress in their Scout leadership training, this is to ensure that they are completing the training and to ensure that relevant and appropriate support is offered to them.

Data is further processed as part of the annual national Scout census in order to provide statistical information on the reach of Scouting across the UK and helps to facilitate appropriate insurance and resources.

It is also processed as part of the safeguarding procedures when DBS checks are repeated at 5 yearly intervals.

Adult data is also processed to allow communication with them to provide information they may need as part of their role including the advertisement of meetings and activities that they and/or their sections may wish to participate in.

Adult names are recorded in minutes of meetings to register their attendance at such a meeting along with any particular proposals they have made at such meetings.

As all safeguarding incidents within the District must be reported to the District Commissioner for referral to the Scout Association safeguarding team by definition the District collects data relating to safeguarding incidents involving volunteers. This data is collected to ensure that the incident is recorded and dealt with by the necessary external agencies.

The communications team collect driving license information from team members who are to drive the team van. This information is collected so that the team can provide accurate information (particularly driving entitlements and points on license) to the insurance company about each driver to ensure full and proper insurance and to ensure that team members are only asked to drive vehicles for which they hold the appropriate license.

Lastly, adult data is from time to time collected and processed to facilitate trips and other District led events.

b) To facilitate their child's membership of Scouting

When a parent submits a 'want to join' enquiry for their child we collect and process data about the parent in order to be able to contact them regarding their child/enquiry.

We also occasionally hold bank details of parents, this is not necessarily through direct collection but is present on the bottom of cheques that are used to make various payments either for events or for purchases via the District shop.

Others

a) To facilitate a campsite booking

When a booking for Pybus Scout Campsite is submitted, we collect and process data about the person/organisation making the booking. This is to ensure that we are able to contact them regarding their booking.

b) To facilitate a communications team booking

When an event organiser makes a booking we collect and process data about the person making a booking (this data may be retained from a previous booking and not collected again). This is to ensure that we are able to contact them regarding their booking.

c) To provide event control services

To provide event control services, we are from time to time, given sensitive personal data by event organisers. We hold this data for the purposes of being able to provide assistance in the event of an incident during the event. This data is provided by the event organiser at the start of the event and returned to them at the end of the event.

From time to time we also receive personal data of other marshals working on the event so as they can be contacted if required.

In addition to this we also collate a list of incidents during an event, this involves collection of details about the individual involved along with the nature of the incident.

d) To protect District property and assets and safeguard campsite users

CCTV is in operation on Pybus Scout Campsite for the protection of District property and assets and to assist in the safeguarding of all users of the site. We use the data collected by CCTV solely in the event of an crime or incident occurring in order to help identify a criminal or establish the circumstances surrounding and event.

Categories of Personal Data Held

*Note: * denotes that special category data is included in the collection*

Person Type	Purpose of Processing	Category of Individual	Categories of Personal Data	Who has access to this data?	Data storage	Recipients of that Data
Young Person	Adding name to waiting list	Potential member	• Name • Gender • DOB • Address • Phone number • Parent's name	District waiting list secretary	• Spreadsheet (Memory Stick) • Paper form • Email (GSuite)	None
Young person	Facilitation of membership of a Scout group	New member	• Name • Gender • DOB • Address • Phone number	District waiting list secretary passes details to those given as recipients	• Email (GSuite and other personal providers) • Paper form	The Group Scout Leader/Section Leader of the receiving Scout Group/Section
Young person (All) *	National Scout census and provision of insurance and resources	Existing Member	• DOB • Gender • Nationality • Additional needs	District census co-ordinator/s (+ Explorer Scout Leaders for Explorer Scouts)	• Paper form • Spreadsheet	Cleveland County Scouts
Young person*	Provision of trips and other District led activities	Existing Member	• Name • Gender • DOB • Emergency contact details • Health information	Event leader	• Paper form • Spreadsheet	Internal events team

Person Type	Purpose of Processing	Category of Individual	Categories of Personal Data	Who has access to this data?	Data storage	Recipients of that Data
Young person (Explorer Scouts and Young Leaders) *	Facilitation of membership of an Explorer Scout or Young Leader unit	New member	• Name • Address • DOB • Phone number • Doctors details • Emergency contact details • Health information	Explorer Scout Leaders or Young Leader Unit Leaders	• Spreadsheet • Paper form • Online Scout Manager	None
Young person (Explorer Scouts and Young Leaders) *	Provision of camps, trips and other activities	Existing Member	• Name • Gender • DOB • Emergency contact details • Health information	Explorer Scout Leaders or Young Leader Unit Leaders	• Paper forms • Email	None
Young person*	The recording and reporting of accidents and injuries	Existing Member	• Name • Accident/injury details • Any relevant health information	• Event leader/first aider (for District led events) • Explorer Scout Leader (in the case of Explorer Scouts) • Young Leader Unit Leader (in the case of Young Leaders)	• Paper form	The Scout Association (in cases where professional medical care has been sought)

Person Type	Purpose of Processing	Category of Individual	Categories of Personal Data	Who has access to this data?	Data storage	Recipients of that Data
Young Person	The recording and management of safeguarding incidents	Existing Member	• Name • Gender • DOB • Contact details • Incident details	• District Commissioner • Referring Leader (initially)	• Paper form • Email • Electronic form	• The Scout Association safeguarding team • External agencies as required
Adult	Adding child's name to waiting list	Parent of potential member	• Name • Address • Phone number • Email address • Child's name	District waiting list secretary	• Spreadsheet • Paper form • Email	None
Adult	Facilitation of child's membership of a Scout group	Parent of new member	• Name • Phone number • Email address • Child's name	District waiting list secretary passes details to those given as recipients	• Email • Paper form	The Group Scout Leader/Section Leader of the receiving Scout Group/Section
Adult	Making payments for Scouting activities or shop purchases	Parent of Existing member	• Name • Bank account details	• Event leader • Explorer Scout Leader • District shop manager • District Treasurer	• Paper form - cheque	Bank
Adult	Joining Scouting	New member	• Name • Phone number • Email address • Address • Gender • DOB	• District appointments secretary • District commissioner • Group Scout Leader	• Paper form • GSuite • Compass	• Compass/The Scout Association • The receiving Scout Group/Section

Person Type	Purpose of Processing	Category of Individual	Categories of Personal Data	Who has access to this data?	Data storage	Recipients of that Data
			• More details can be recorded on compass but the District does not routinely collect these	• District Administrator • Group Administrator		
Adult	Joining Scouting	New member	• Name • Phone number • Email address • Address • Nationality • DOB • ID Document details (passport number, driving license number etc)	• Person checking ID as part of DBS process • Person entering details onto Atlantic Data as part of DBS process (if not the same persona as above)	• Paper form • Atlantic data	• Atlantic Data • DBS
Adult	Joining Scouting	New member	Criminal convictions	District Commissioner	• Paper form	Shared internally with a small selection of appointments committee members to determine suitability
Adult	National Scout census and provision of insurance and resources	Existing member	• DOB • Gender • Nationality • Additional needs	District census co-ordinator/s	• Paper form • Spreadsheet	The Scout Association

Person Type	Purpose of Processing	Category of Individual	Categories of Personal Data	Who has access to this data?	Data storage	Recipients of that Data
Adult	Renewal of DBS check	Existing member	• Name • Phone number • Email address • Address • Nationality • DOB ID Document details (passport number, driving license number etc)	• Person checking ID as part of DBS process • Person entering details onto Atlantic Data as part of DBS process (if not the same person as above)	• Paper form • Atlantic data	• Atlantic Data • DBS
Adult	Renewal of DBS check	Existing member	Criminal convictions	District Commissioner	• Paper form	Shared internally with a small selection of appointments committee members to determine ongoing suitability
Adult	Recording a members attendance and contributions to a meeting	Existing member	Name	• Attendees of the meeting • District Commissioner	• Google Drive • Email	• Attendees of the meeting • Those entitled to attend the meeting
Adult	Recording a members training progress	Existing member	• Name • Scout Group • Modules completed	District Training Manager	• Spreadsheet	None
Adult	Recording of DBS expiry dates	Existing member	• Name • Role • Scout Group • DBS check issue date	District appointments secretary	• Spreadsheet	None

Person Type	Purpose of Processing	Category of Individual	Categories of Personal Data	Who has access to this data?	Data storage	Recipients of that Data
			• DBS check expiry date			
Adult *	Provision of trips and other District led events	Existing member	• Name • Gender • DOB • Emergency contact details • Health information	Event leader	• Paper form • Spreadsheet	Internal events team
Adult *	The recording and reporting of accidents and injuries	Existing Member	• Name • Accident/injury details • Any relevant health information	• Event leader/first aider (for District led events) • Communications team manager (for incidents involving the communications team)	• Paper form before being scanned to Google Drive and the paper destroyed	The Scout Association (in cases where professional medical care has been sought)
Adult	The recording and management of safeguarding incidents	Existing Member	• Name • Gender • DOB • Contact details • Incident details	• District Commissioner • Referring Leader (initially)	• Paper form • Email • Electronic form	• The Scout Association safeguarding team • External agencies as required

Person Type	Purpose of Processing	Category of Individual	Categories of Personal Data	Who has access to this data?	Data storage	Recipients of that Data
Adult	Checking driving license entitlements and endorsements prior to driving the communications team van	Existing Member	• Name • Driving license details	Communications team manager	• Spreadsheet	Endorsements are passed to insurance company
Others	Campsite bookings	Non-member	• Name • Address • Email address • Telephone number(s)	• Pybus booking secretary • Campsite wardens (name, email and telephone number(s) only)	• Paper form • Google Sheets • Google Calendar	None
Others	Communications team bookings	Non-member	• Name • Address • Email address • Telephone number(s)	• Communications team manager	• Spreadsheet • Email • Mobile phone • OneDrive	None
Others *	Event control	Non-member	• Name • Emergency contact details • Health information	• Communications team members • Communications team manager	• Paper forms	Provided by and returned to event organisers

Person Type	Purpose of Processing	Category of Individual	Categories of Personal Data	Who has access to this data?	Data storage	Recipients of that Data
Others	Event control	Non-member marshal	• Name • Phone number	• Communications team members • Communications team manager	• Paper form	None
Others	Event incident logging	Non-member	• Name • Nature of incident • Disposal method	• Communications team members • Communications team manager	• Spreadsheet • OneDrive	Event organiser
All	Protection of District property and assets and safeguarding campsite users	Members and non-members	• Image	• District Commissioner • Nominated second person (shown in CCTV policy)	• CCTV DVR	Police – in the event of a crime being comitted

Transfer of Data Outside of the UK

The District does not consciously transfer any data outside of the UK. All third-party processors are either based in the UK or (in the case of Google, Microsoft and Drop Box) fully GDPR compliant with regard to transfer of data outside of the UK.

Retention Schedules

Data type	Retention period	Storage media & Location
Waiting list data	Waiting list data is retained for a period of 3 years from the young person being offered a place in a group. This is to ensure that should there be a query before the young person would transfer to the waiting list for the next section we are able to identify when and where they were placed so that they are not disadvantaged if there has been an error. The data held is reduced as far as is practicable.	Spreadsheet – Waiting list secretary's home
Census data	Data held as part of the Scout census is held until the District Census return has been submitted and has been approved by the County team. At this point all data held solely for this purpose is deleted or destroyed	• Spreadsheet – District census co-ordinator's home • Paper form – District census co-ordinator's home
Adult member data	Data is retained on Compass until an adult member's role is marked as closed at which point this becomes inaccessible to any person within the District and the retention policy of the Scout Association should be consulted for further details.	Online membership system - Compass
Adult criminal record history	Data is retained until appointments committee has considered the suitability of an applicant for an appointment in the District after which the data is destroyed.	Paper form – District Commissioner's Home
Young person and adult trip or event data	Trip or event data is held for a period of no more than 3 months from the end of the event.	Paper form – Event leader's home
Explorer Scout and Young Leader membership data	Membership data is held for a period of no more than 3 years before being deleted and/or destroyed. This ensures that should the young person wish to re-join we still have the details of the progress they have already made within the section.	• Spreadsheet – Explorer Scout Leader's computer • Paper form – Explorer Scout Leader's home • Online membership system – Online Scout Manager
Safeguarding incident data	This data is collected at the time that the incident is reported and held until such time as the Scout Association safeguarding team advise that the incident has been resolved and/or closed.	• Paper form – reporting volunteer's home

		• Paper form – District Commissioner's home • Email – GSuite • Electronic form – District Commissioner's laptop or GSuite
Accident/injury records	To comply with relevant legislation, records of accidents/injuries will be held for a period of up to three years from the incident date (in the case of adults) and up until the individual affected reaches the age of 21 (in the case of young people) before being deleted or destroyed.	Electronic form - GSuite
Gift Aid	To comply with HMRC and Charity Commission regulations all gift aid claim forms are retained for a period of 6 years from the end of the accounting period to which they relate, after such time the data is deleted or destroyed.	• Paper form – District gift aid co-ordinator's home (short term storage) • Paper form – Pybus (long term storage)
Bank details	Bank account details are only held until such time as the cheque that they are stored on is paid into the relevant bank account.	Paper form – receiving volunteer's home
Adult driving license data	Driving license data is held for the time period an adult is a member of the communications team or has been appointed to drive a team vehicle	Spreadsheet – Communications team manager's laptop
Bookings data	Bookings data is held for a period of 3 years in electronic format in order to help identify booking trends and streamlining the repeat booking process. Some bookings data is held alongside the District accounts for a period of 7 years for the purposes of identifying a source of income in accordance with Charity Commission regulations.	• GSuite (Google Drive and Google Calendar) • Paper Form - Pybus
Event control event participant data	Participant data is held solely for the duration of the event and is returned to the event organiser for disposal at the end of the event.	Various forms – Communications team event base (Van/Trailer/Other)
Event control non-member marshal data	The details of non-member marshals are held for the duration of the relevant event and then deleted or destroyed.	Spreadsheet – Communications team manager's laptop
Event incident logs	Incident logs are sent to the event organisers directly after each event however will also be retained by us for a period of no more than 3 years so that we still have access to the data in the event of any queries about the action we took or the support we provided.	Communications team One Drive
CCTV images	CCTV images are recorded onto a 1TB hard drive, these images a retained until the drive is full and it starts to	CCTV DVR - Pybus

	overwrite the oldest footage (it is estimated that this equates to 30 days of footage)	

Technical and Organisational Security Measures

GSuite

GSuite is used as an email provider (Gmail), office application provider (Google Docs), and cloud storage system (Google Drive). It is provided by Google and is one of the market leading providers of such services.

All GSuite products use SSL encryption. All data recorded within GSuite (including emails) is stored securely and is encrypted. Emails sent externally to the GSuite system are potentially sent in plain text and the contents could be viewed if intercepted.

Access to GSuite products is controlled using rights based access controls. This means that only users with the appropriate access rights can access documents, data and services relevant to their role. All users are required to have a complex password of at least 8 characters in length – this can be increased in the admin console. Whilst no central facility exists to enforce a mixture of alphanumeric characters and special characters password strength can be monitored and as of 9th April 2018 all users are showing as having strong passwords.

Whilst GSuite can generally be assumed to be a secure means of data storage given its own encryption systems, password policy and back-up systems, it could be a target of large scale cyber-attacks.

One Drive

One Drive is a cloud storage platform provided by Microsoft.

Users are required to have a password of at least 8 characters in length and contain at least two of the following, upper case letters, lower case letters, numbers and symbols.

One Drive can generally be assumed to be a secure means of data storage given its own encryption systems, password policy and back-up systems, it could however also be the target of large scale cyber-attacks.

Drop Box

Drop Box is a stand-alone cloud storage platform.

Users are required to have a password of at least 6 characters in length.

Drop Box can generally be assumed to be a secure means of data storage given its own encryption systems, password policy and back-up systems, it could however also be the target of large scale cyber-attacks.

Facebook

The District makes use of closed Facebook groups. These Facebook groups are open only to volunteers and supporters of the District and as a closed group the content is only available to these group members. Visible to the public is simply a list of the people who are members of the group, this is controlled by Facebook and the District has no ability to change this. Facebook requires all users to have an individual username (usually tied to the user's email address) and a password to be able to log in. No sensitive personal information is posted on the Districts Facebook groups, only users names and from time to time event photographs are visible to group members.

Paper Forms

Paper forms are used to collect a variety of personal data, the retention and storage of these forms varies depending upon their purpose. Paper forms in long term storage are in stored in a locked cupboard in which only a given number of people have keys to access. Those which require regular access are stored with the person who requires access and the District recommends that they are stored within a locked container in the domestic environment.

Paper forms containing information about an adults criminal convictions are destroyed after use – either by means of shredding through a shredder or by burning.

The main risk to the security of paper based records is loss or theft. With this method of data storage the ability to search is incredibly manual and the ability to update very difficult both of which will take up large amounts of valuable volunteer time.

Spreadsheets and other electronic forms

Spreadsheets and other electronic formats are used to hold all manner of data and are stored in a variety of different places across the District. The District recommends that all such data stored outside of GSuite is password protected or stored on encrypted media *(ideally both)*.

The biggest risk to the security of data stored in electronic form is the storage media that it is stored on. All data stored in electronic form should be stored in encrypted form and on encrypted media. Furthermore, access and amendment is not logged to a particular user.

Compass

Compass is provided by The Scout Association for the purposes of collecting and storing all personal information about adult volunteers. The product uses SSL encryption and requires a username and password (which must be a mixture of upper and lowercase alphanumeric characters and special characters). Usernames and passwords are unique to individual users and each user has permission to view only the data that their role permits.

The Scout Association also act as a data controller with respect to adult volunteer data.

Atlantic Data

Atlantic Data is a system provided by The Scout Association for the purposes of applying for DBS checks for adult volunteers. The product uses SSL encryption and requires a username and password (which must be a mixture of upper and lowercase alphanumeric characters and special characters). Passwords must be changed every 90 days and users cannot reuse a previous password. Usernames and passwords are unique to individual users and each user has permission to view/enter only the data that their role permits.

The Scout Association also act as a data controller with respect to adult volunteer data.

Online Scout Manager (OSM)

Online Scout Manager is a management information system specifically designed for Scout leaders. It is able to store all records about a person's membership of a Scout Group. The product uses SSL encryption and requires a username and complex password (which must be at least eight characters containing a mixture of at least two types of character). A security question is built in as a second layer of authentication when a user first logs on from a new device.

Access to OSM is controlled using rights based access controls. This means that users can only access or amend the data that is relevant to their role.

A data sharing agreement is in place with the Scout Association which allows their safeguarding team to access the personal details of members directly as a last resort if the information cannot be obtained through the usual channels. Data accessed in this way is logged within OSMs audit trail.

The product is fully GDPR complainant and publishes their own detailed data protection information on their website "https://www.onlinescoutmanager.co.uk/security.html"

Lawful Basis for Processing

Process	Purpose of processing	Category of personal information	Data captured to drive categorisation	Retention policy	Lawful basis for processing	Approved by and when?
Young member joining	A young person's details are collected as part of the joining process	Personal data	• Name • Gender • DOB • Address • Phone number • Parent's name	Waiting list data is retained for a period of no more than 3 years after the young person has been allocated a place in a group before being deleted and/or destroyed	Consent – consent has been given by the subject(s parents) to process the data	The Trustees 17/9/18
Young member Scout Census	A young person's details are shared as part of the national Scout census	Sensitive personal data	• DOB • Gender • Nationality • Additional needs	Data is held until the District census return has been completed and approved by the County team before being deleted and/or destroyed	Legitimate interests – this data is required to ensure that: • Insurance cover is in place • Appropriate support is offered to adult volunteers to help them support young people form particular nations or with additional needs	The Trustees 17/9/18
Explorer Scout and Young Leader joining	An Explorer Scout or Young Leader's details are collected as part of the joining process	Sensitive personal data	• Name • Address • DOB • Phone number • Doctors details	Data is held for a period three years after the Explorer Scout or Young Leader leaves the section.	• Consent – consent has been given by the subject(s parents) to process the data • Vital Interests – health information is necessary	The Trustees 17/9/18

Process	Purpose of processing	Category of personal information	Data captured to drive categorisation	Retention policy	Lawful basis for processing	Approved by and when?
			• Emergency contact details • Health information		to ensure that the subjects needs are taken into account when planning an event and that they are helped appropriately in the case of an accident or injury	
Explorer Scout and Young Leader camps, trips and events	An Explorer Scout or Young Leader's details are collected to ensure leaders have the most up to date information for camps, trips and activities	Sensitive personal data	• Name • Address • DOB • Phone number • Doctors details • Emergency contact details • Health information	Data is held for the duration of the event and is destroyed no more than three months from the date of the end of the event	• Consent – consent has been given by the subject(s parents) to process the data • Vital Interests – health information is necessary to ensure that the subjects needs are taken into account when planning an event and that they are helped appropriately in the case of an accident or injury	The Trustees 17/9/18
Safeguarding incident management	Details of any safeguarding incidents are collected so that they can be referred to the Scout Association safeguarding team	Sensitive personal data	• Names of persons involved • Nature of incident • Contact details for persons involved (and/or their parents)	Data is held until such time as the Scout Association safeguarding time advise that incident has been resolved/closed	• Vital interests – the collection of this data is necessary to protect the interests of the individuals involved and ensure appropriate action is taken	The Trustees 17/9/18

Process	Purpose of processing	Category of personal information	Data captured to drive categorisation	Retention policy	Lawful basis for processing	Approved by and when?
	for investigation and further referral to the necessary external organisations		• Other details as relevant to the incident		• Legitimate interests – it is necessary to collect this data in order to safeguard the other people in our care from any impact the incident may have upon them • Legal obligation – in the event that the incident involves criminal proceedings we may be required to provide this information as evidence to the necessary authorities	
Accident or injury management	In the event of an accident or injury details are recorded of the incident, the actions taken and (in the event of professional medical treatment being required) passed to the Scout Association as our insurers	Sensitive personal data	• Names of persons involved • Details of accident or injury • Relevant health information (i.e. prior conditions that may have had an effect)	Data is held for a period of three years from the date of the incident or until the 21st birthday of the individual involved whichever is the later.	• Vital interests – it is in the vital interests of the person involved in the incident to ensure that the nature of the incident and the actions taken are recorded. • Legitimate interests – it is in the legitimate interests of the District to ensure that accidents and the actions taken are recorded so as to help in	The Trustees 17/9/18

Process	Purpose of processing	Category of personal information	Data captured to drive categorisation	Retention policy	Lawful basis for processing	Approved by and when?
					the event of any claim made against the District	
Gift aid claim	To facilitate the District's ability to claim gift aid on donations made	Personal data	• Name • Address	Gift aid claim data is held for a period of 6 years from the end of the accounting period to which the claim relates.	• Consent – the subject has given consent to process the data	The Trustees 17/9/18
Cheque payments	To make payments to the District	Personal data	• Name • Bank account details	Data is retained until such time as the cheque is paid into the relevant bank account at which point we no longer hold the data	• Consent – the subject has given us consent by choosing this method of payment • Legitimate interests – we need to take payments in order to be able to provide products or events	The Trustees 17/9/18
Adult volunteer joining	Adult volunteer details are collected as part of the joining process	Sensitive personal data	• Name • Phone number • Email address • Address • Nationality • DOB	Data is accessible to the District on Compass until the adult leaves the movement and their role(s) are marked as closed	• Consent – the subject has given consent to process the data • Contract – certain steps must be taken before an adult can become a member	The Trustees 17/9/18

Process	Purpose of processing	Category of personal information	Data captured to drive categorisation	Retention policy	Lawful basis for processing	Approved by and when?
Adult appointments	Adult volunteers criminal offence data is shared with the District by the Scout Association so that an appointments committee can determine that adults suitability to be a volunteer	Criminal offence data	• Name • Criminal offence data	Data is held until appointment is approved or rejected and then destroyed either by way of shredding or burning	Legitimate interests - It is necessary to process this data to safeguard the young people in our care	The Trustees 17/9/18
Adult volunteer wishing to drive communications team van	An adults driving license is checked before they are added to the insurance to be able to drive the communications team van to ensure they have a valid license, establish their driving license entitlements and the number of penalty points that they hold (if any) so as to be able to provide accurate information	Sensitive personal data	• Name • Address • Driving license data	Driving license data is held for the time period an adult is a member of the communications team or has been appointed to drive a team vehicle	• Legal obligation – drivers are legally obliged to hold a valid driving license with the relevant entitlements and hold at least 3rd party insurance before being able to drive a vehicle on the public highway. • Legitimate interests – it is necessary to process this information in order to gain appropriate insurance for the member concerned to drive the van	The Trustees 17/9/18

Process	Purpose of processing	Category of personal information	Data captured to drive categorisation	Retention policy	Lawful basis for processing	Approved by and when?
	to the insurance company					
Events management	Young person and adult details are collected to facilitate their attendance at an event	Sensitive personal data	• Name • Address • DOB • Emergency contact details • Health information	Data is held for the duration of the event and is destroyed no more than three months from the date of the end of the event	• Consent – the subject (or their parent) is providing consent for the District to process this data for the purposes of an event • Vital interests – health information is necessary to ensure that the subjects needs are taken into account when planning an event and that they are helped appropriately in the case of an accident or injury	The Trustees 17/9/18
Pybus Campsite or Communications Team Bookings	An adult's details are collected to process a campsite or communications team booking	Personal data	• Name • Address • Email address • Telephone number(s)	Data is held for a period of no more than 3 years in electronic form however paper copies of booking data are held with the District accounts for a period of 7 years in line with Charity Commission regulations.	Contract – It is necessary collect and process this information for the District to be able to provide a service to the subject	The Trustees 17/9/18
Event Control	Personal details are held in order to be able to provide	Sensitive personal data	• Name • Emergency contact details	Data is held for the duration of the event and then returned to the event	• Vital interests – it is necessary to hold this information to ensure that	The Trustees 17/9/18

Process	Purpose of processing	Category of personal information	Data captured to drive categorisation	Retention policy	Lawful basis for processing	Approved by and when?
	support and assistance in the event of an accident or injury		• Health information	organiser for them to dispose of appropriately	prompt and appropriate support can be offered to an individual by our team should they be involved in and incident or accident • Contract – it is necessary to hold this information in order to be able to provide a service the event organiser	
Event control	Personal details of non-member marshals are held in order to communicate with them during an event	Personal data	• Name • Telephone number	These details are retained for the duration of the relevant event and then deleted/destroyed	Legitimate interests – the event control team need to be able to communicate with all marshals working on an event to communicate vital information to them if required	The Trustees 17/9/18
CCTV	To protect District property and assets and aid the safeguarding of all campsite users.	Personal Data	• Image	CCTV images are retained until such time as the footage is overwritten due to the DVR hard drive being full. It is estimated that this is a 30 day cycle.	Legitimate interests – CCTV imagery is required in order to allow the District to identify the persons involved in any criminal acts or to establish the circumstances surrounding any other incident which occurs whilst there is no one on site. This	The Trustees 17/9/18

Process	Purpose of processing	Category of personal information	Data captured to drive categorisation	Retention policy	Lawful basis for processing	Approved by and when?
					cannot be achieved through any means other than CCTV	

Risk Register

Area to which risk applies	Owner of risk and its mitigation	Description of risk	Risk rating (based on impact of risk)	Description of recommended management or mitigation of risk	Cost impact	Mitigation option chosen (colour indicates residual risk)
District	District Executive Committee	Maintenance of lawful processing records – this is to be an ongoing effort	Medium	Review all data capture systems and develop a system for maintaining records of lawful processing	None	Initial records of data processing records created as per this document. To be reviewed at 2 monthly intervals for first year with this period reviewed in 1 year
• District • Explorers • Communications Team	• District Executive Committee • Explorer Leaders • Communications team manager	District owned computer equipment holding personal sensitive data do not have strong passwords	High	Implement passwords on District owned devices	None	District owned equipment to have passwords applied
• District • Explorers • Communications Team	• District Executive Committee • Explorer Leaders • Communications team manager	Privately owned computer equipment holding personal sensitive data do not have strong passwords	High	Recommend that all privately owned devices holding personal sensitive data are protected by a strong password.	None	Recommendation made to all members of the District team holding personal data to protect personal devices with a strong password
• District • Explorers • Communications Team	• District Executive Committee • Explorer Leaders	District owned computer equipment holding personal sensitive data has no local encryption	High	Encrypt District owned devices either by upgrading to newer professional grade equipment or by the use of a third party application.	None to Medium	District owned devices to be encrypted

Area to which risk applies	Owner of risk and its mitigation	Description of risk	Risk rating (based on impact of risk)	Description of recommended management or mitigation of risk	Cost impact	Mitigation option chosen (colour indicates residual risk)
	• Communications team manager					
• District • Explorers • Communications Team	• District Executive Committee • Explorer Leaders • Communications team manager	Privately owned computer equipment holding personal sensitive data has no local encryption	High	Recommend that all privately owned devices are encrypted using the tools built into the Windows and Mac operating systems or by using a third party application.	None	Recommendation made to all members of the District team holding personal data to encrypt personal devices using appropriate software tools
All levels	District Executive Committee and District Team	Ensuring that all adults handling personal data have sufficient technical skill to ensure electronic data is secured in storage and in transit	Medium	• Provide training for adults on appropriate data protection techniques. • Provide training in the use of products such as GSuite to aid data protection.	Low	Training session to be arranged to highlight the importance of data protection and the technical measures available for data protection.
• District • Explorers • Communications Team	• District Executive Committee • Explorer Leaders • Communications team manager	Paper based records are held in a variety of locations	High	Review use of paper records. Could these be entirely replaced with an electronic system? Could paper forms be scanned and stored in cloud storage with paper forms being destroyed after scanning?	Low	Long term review of the use of paper records

Area to which risk applies	Owner of risk and its mitigation	Description of risk	Risk rating (based on impact of risk)	Description of recommended management or mitigation of risk	Cost impact	Mitigation option chosen (colour indicates residual risk)
• District • Explorers • Communications Team	• District Executive Committee • Explorer Leaders • Communications team manager	Privacy policies at data capture point not transparent enough or ability to opt in to further communication omitted	High	Develop and circulate a range of standard privacy policy notices that can be amended to suit various data capture points	None	Review and trial privacy notices range of standard amendable notices
• District • Explorers • Communications Team	• District Executive Committee • Explorer Leaders • Communications team manager	Data captured is kept forever with no defined policies for retention	High	Set retention policies and ensure these are communicated to all relevant parties	None	Retention policies have been set and approved by the trustees as given elsewhere in this document. These are communicated to all and reduce this risk to low.
District	District Executive Committee	Multiple data sources mean that it will be difficult to delete, change or supply personal data on the request of the data subject	Medium	Aim for a standard model of data storage taking privacy and ease of use into consideration	Low	Long term data storage review – increase use of GSuite

Automated Decision Making

The District does not use any automated decision making systems. The only automated process is within Atlantic Data whereby the person inputting the ID documents selects from a list the ID that the applicant has provided and when adequate ID has been selected the process is allowed to continue; this is simply a convenience feature and not a decision that is made about the applicant.

Sources of Personal Data

All personal data in the categories of young persons and adults is provided by the individual (or their parent in the case of a young person).

In the case of others, the source varies:

- For bookings (both campsite and communications team) the data is provided by the individual
- For event control services, the data is provided by the event organiser who has collected the information according to their own data protection policies and act as a data controller in this regard.
- CCTV imagery is captured automatically when a person moves past a CCTV camera on Pybus campsite, land owned by the District. Whilst cameras have been sited to cover specific areas of the site, they do also capture the public rights of way that runs across the land.

Individual's Rights

The right to be informed

Data subjects have the right to be informed about the collection and use of their data. The District gives clear information regarding, the purpose for processing, the retention period and who the data will be shared with at the point of collection.

The right to access

Data subjects have the right to access their personal data and/or confirm that their data is being processed. The District has a procedure for dealing with Subject Access Requests, this is detailed later in this document.

The right to rectification

Data subjects have the right to request that inaccurate personal data be corrected or completed where incomplete. This request can be made verbally or in writing.

The right to erasure

Data subjects have "the right to be forgotten" or to have their personal data erased, this request can again be made verbally or in writing. This right can be exercised if:

- the personal data is no longer necessary for which we originally collected it
- the data subject withdraws their consent when consent is the only legal basis on which we collected the data

- where legitimate interests in the legal basis on which we collected the data and this interest no longer exists

The right to restrict processing

Individuals have the right to restrict the processing of their personal data. In these circumstances, we are permitted to store the data but not use it. This request can be made in writing or verbally. This right only applies in the following circumstances:

- The data subject is contesting the accuracy of their data and we are verifying the accuracy
- The data has been unlawfully processed and the individual opposes erasure and requests restriction instead
- We no longer need the data but the data subject needs us to keep it in order to establish, exercise or defend a legal claim.
- The data subject has objected to our processing of their data under Article 21(1) and we are considering whether our legitimate grounds override those of the data subject

In order to restrict processing we will ensure that the request is noted and that any data we hold in paper form is moved to one side so that it is not processed with other data. We will ensure that electronic data is filed together and that access is restricted to a limited set of users.

The right to object

Data subjects have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

We will consider all objections however we may continue to process the data if we can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or the processing is for the exercise or defence of a legal claim. If an objection is upheld we will cease to process the individual's data.

Data Breach Response Plan

The District Executive Committee is responsible for the security, integrity and confidentiality of all the data it holds. Under the GDPR it is obliged to keep that data safe, secure at all times. They are also responsible for the management of data breaches.

Any person who knows or suspects that a breach of data security has occurred should report the breach immediately according to this plan. It is vital that action is taken promptly in the event of any actual, potential or suspected breaches of data security or confidentiality so as to avoid the risk of harm to young people or adult volunteers, damage to operations, financial, legal and reputational costs.

Defining a data breach

A data breach is any event that has the potential to affect the confidentiality, integrity or availability of personal data held by the District in any format. They can happen for a number of reasons including:

- Disclosure of data to unauthorised individuals
- Loss or theft of portable devices containing identifiable information
- Loss or theft of paper records
- Inappropriate access controls which allow unauthorised use of information
- Suspected breach of IT security
- Attempts to gain unauthorised access to IT systems
- Records altered or deleted without the authorisation of the data owner
- Viruses or other security attacks to computer systems
- Breaches of physical security
- Confidential information left unlocked in accessible areas
- Insecure disposal of confidential paper waste
- IT equipment left unattended whilst logged in without taking steps to prevent others accessing information
- Publication of confidential data on the internet in error and accidental disclosure of passwords
- Misdirected emails containing personal data

The response plan

This plan applies to all personal data created or received by the District in any format regardless of where it is used and in the case of IT related breaches applies whether the data is stored on District owned devices or systems or personal devices.

Identification and Initial Assessment

- Breach notification form completed
- Identify:
  - What personal data is involved in the breach
  - The cause of breach
  - Extent of breach (how many individuals are affected)
  - The harms that could potentially be casued to individuals due to the breach
  - How the breach can be contained
  - Determine severity of incident (using data breach severity form)

Containment and Recovery

- Establish who needs to be made aware of the breach and inform them of what they are expected to do to contain it (for example find a lost piece of equipment or change locks etc)
- Establish if anything can be done to recover any losses and limit the damage that the breach can cause (i.e. recovery of equipment or records and the use of back-ups to restore lost or damaged data)
- Establish if it is appropriate to notify affectd individuals immendiately (i.e. where there is a high risk of serious harm to them)
- Inform the police where appropriate (i.e. if breach involved theft or other criminal actions)

Risk Assessment

- Assess risks and consequences of breach
- What are the risks and potential adverse consequences for the individuals? (safety, reputation, financial loss or a combination?)
- How serious or substatial are the consequences and how likely are they to happen?
- What are the risks to the District (Strategic, legal, financial and reputational)
- Prepare incident report

Notification

- Decide if it is necessary to inform others outside of the Distric of the breach (i.e. parents, affected data subjects, ICO, policy, press via The Scout Association media team, insurers etc)
- What message needs to be communicated? (Description of how and when breach occurred, what data was involved, what action has been taken to respond to risks posed by breach)
- Clear advice given to individuals on steps necessary to protect themselves
- The District Executive Committee is not required to inform the ICO of breaches which result in loss, release or corruption of data but the ICO expect that serious breaches are brought to their attention. (Any such notification should be within 2 days of the breach)

Evaluation and Response

- Review to ensure steps taken during incident were appropirate and identify areas for improvement
- Compile a central record of incidents
- Report on incidents to adult volunteers to identify lessons to be learnt, patterns of incidens and evidence of weaknesses that need to be addressed.
- What action needs to be taken to reduce the risk of future breaches and minimise their impact?
- Do policies and procedures needs to be improved to increase effectiveness of response?
- Are there any weak points in security controls that need to be strengthend?
- Are users aware of the theire responsibilities with regards to information security and are they adequetely trained?

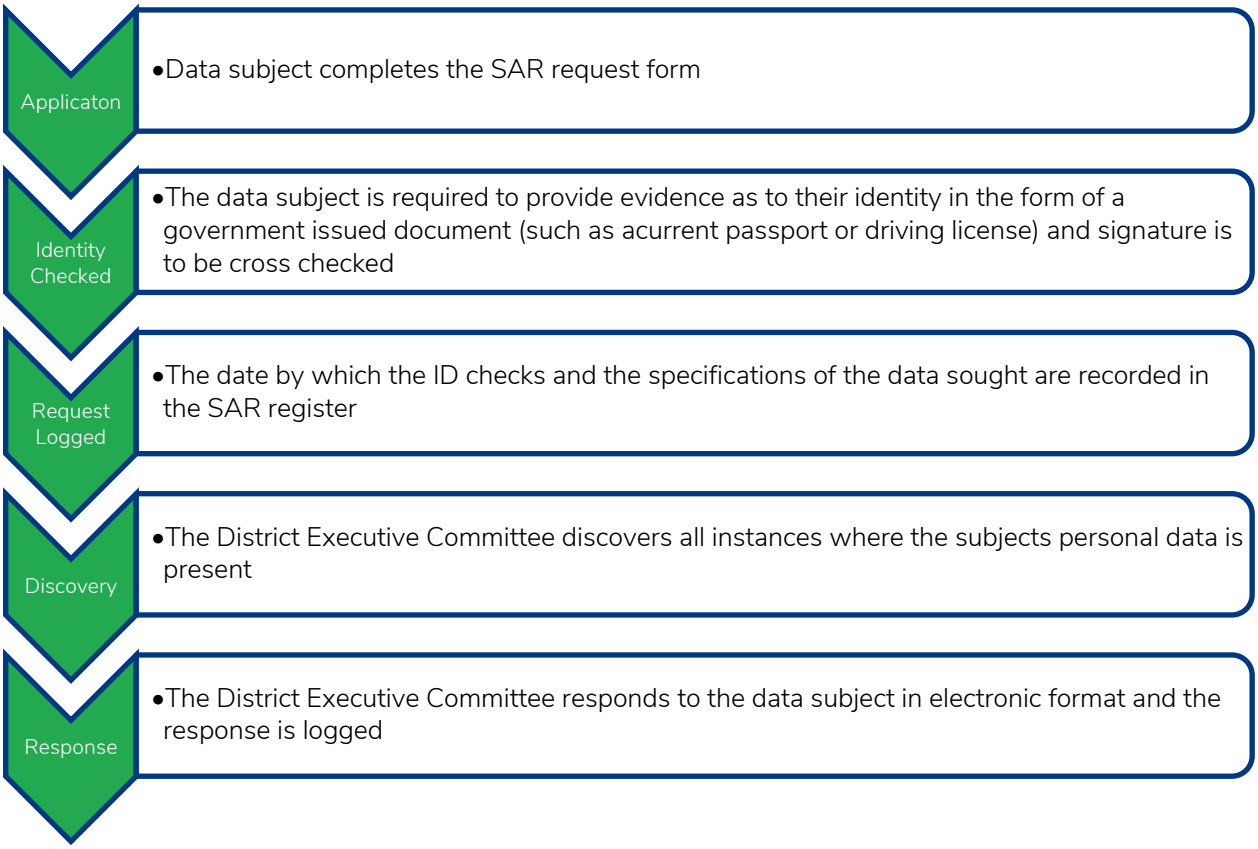
Subject Access Requests

Data subjects have a right to ask for the information we hold on them through the Subject Access Request (SAR) process.

We are not obliged to provide this information if the request falls under any of the following exemptions:

- Crime prevention and detection
- Negotiations with the requester
- Information used for research, historical or statistical purposes
- Information covered by legal professional privilege

The SAR procedure is outlined here:



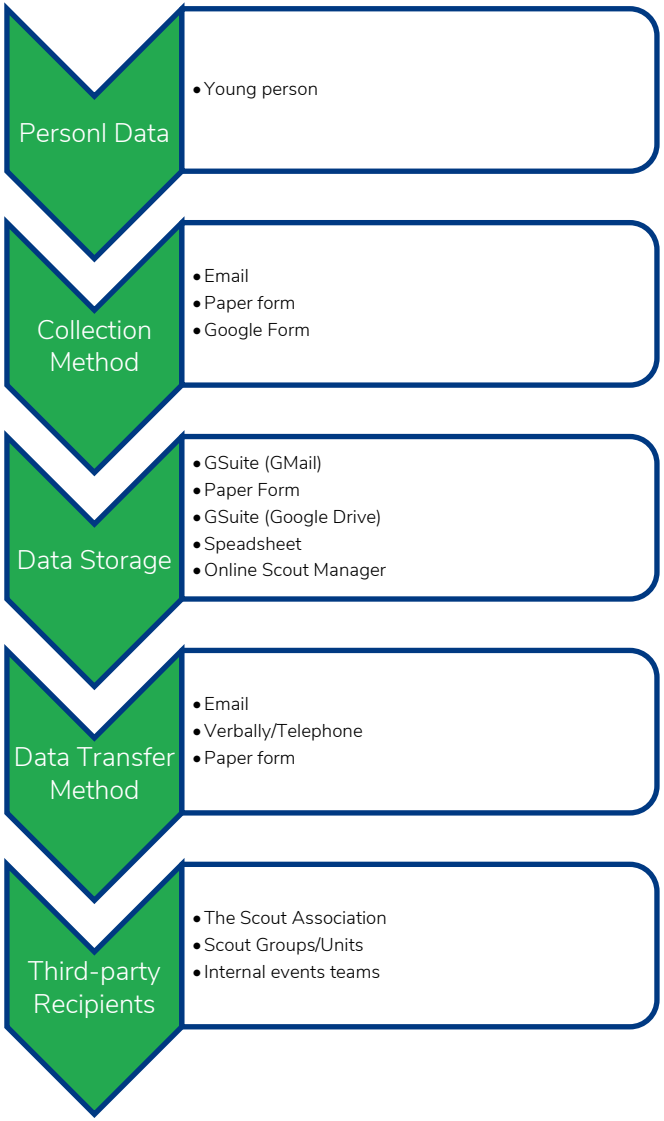
Whilst the District Executive Committee is responsible for handling all SAR's they will require help from other members of the District.

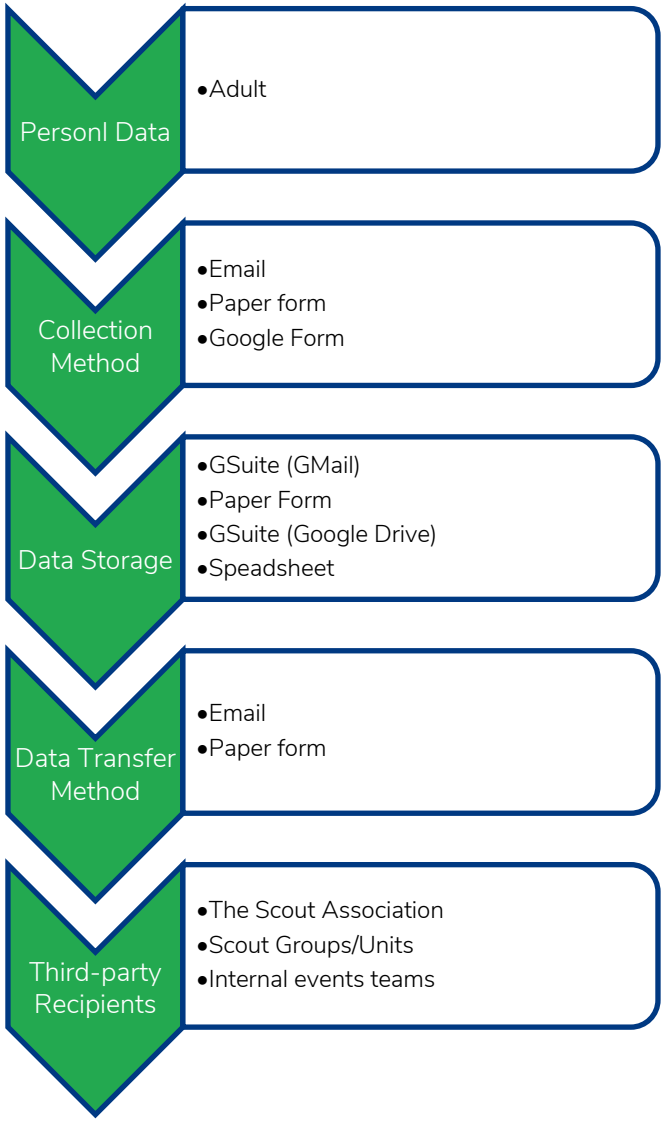
Discovery: the District will collect the data specified by the data subject or search all filling systems (electronic and paper based) in the District.

Response: The District Executive Committee will review all documents provided to identify whether any other third parties are identified within them and omit or redact the third-party information or seek written consent from the third-party for their identity to be shared.

All responses will be provided to the subject in electronic form. The data subject's name, list of items provided and date on which they were provided will be recorded.

Appendix 1


Personl Data
• Young person
Collection Method
• Email
• Paper form
• Google Form
Data Storage
• GSuite (GMail)
• Paper Form
• GSuite (Google Drive)
• Speadsheet
• Online Scout Manager
Data Transfer Method
• Email
• Verbally/Telephone
• Paper form
Third-party Recipients
• The Scout Association
• Scout Groups/Units
• Internal events teams


Personl Data
•Adult
Collection Method
•Email
•Paper form
•Google Form
Data Storage
•GSuite (GMail)
•Paper Form
•GSuite (Google Drive)
•Speadsheet
Data Transfer Method
•Email
•Paper form
Third-party Recipients
•The Scout Association
•Scout Groups/Units
•Internal events teams

Change Log

Version	Change/s	Date Issued
v1.0	Initial draft	17th Sept 2018
v1.1	• Retention policies for safeguarding incident data clarified • References to accident/injury management updated to reflect the move to use GSuite for data storage rather than paper	9th Oct 2019
v1.2	• Addition of references to Online Scout Manager to reflect Explorer Scout units use of the product	13th Dec 2019
v1.3	• Addition of information relating to the OSM and Scout Association data sharing agreement	25th Aug 2020

Registered charity no. 524704