# Clyde Scouts Privacy Policy

Contents

[Introduction 2](#_Toc95743680)

[1. Purpose of this Data Protection policy and what it covers 2](#_Toc95743681)

[2. How to complain 2](#_Toc95743682)

[3. Important definitions 3](#_Toc95743683)

[4. What is personal data? 3](#_Toc95743684)

[5. Data Protection and Scouting 4](#_Toc95743685)

[6. What type of personal data we collect and why? 4](#_Toc95743686)

[6.1 Members and volunteers 4](#_Toc95743687)

[6.2 Trustees and members of the governance structure 5](#_Toc95743688)

[6.3 Donors 5](#_Toc95743689)

[6.4 Customers and visitors 5](#_Toc95743690)

[6.5 Employees (past, present and future) 6](#_Toc95743691)

[6.6 CCTV 6](#_Toc95743692)

[7. The Law 6](#_Toc95743693)

[7.1 Sharing information 8](#_Toc95743694)

[8. Keeping data secure 9](#_Toc95743695)

[9. Responsibilities 10](#_Toc95743696)

[9. 1 Board of Trustees 10](#_Toc95743697)

[9.2 Chief Operating Officer 10](#_Toc95743698)

[9.3 Staff 10](#_Toc95743699)

[9.4 Volunteers, members and local Scouting 11](#_Toc95743700)

[10. Data Retention 11](#_Toc95743701)

[11. Subject Access Request 11](#_Toc95743702)

[11.1 How do we recognise a subject access request (SAR)? 11](#_Toc95743703)

[11.2 What about requests for information about children? 12](#_Toc95743704)

[11.3 What should we consider when responding to a request? 12](#_Toc95743705)

[11.4 Accessing and updating 12](#_Toc95743706)

# Introduction

Clyde Scouts are committed to protecting privacy and personal data. Clyde Scouts are a registered charity in Scotland, registered charity number SC010415, and are members of Scouts Scotland and The Scout Association (TSA).

It is important to note that as Data Controllers, local Scout Groups and Districts are directly responsible for any personal data they process and must therefore ensure that they are aware of their responsibilities under the law.

# Purpose of this Data Protection policy and what it covers

This policy sets out Clyde Scouts’ approach to protecting personal data and explains your rights in relation to how we may process personal data.

Clyde Scouts(“We” in this document) are registered with the Information Commissioner’s Office at the following address:
21 Elmbank Street, Glasgow, G2 4PB.

If you have any questions about this policy, please contact our Chief Operating Officer via email at info@clydescouts.org.uk

We may from time to time make minor changes to this policy and announce any significant changes via our website.

# How to complain

If you have any concerns about our use of your personal information, you can make a complaint to us at info@clydescouts.org.uk.

You can also complain to the ICO if you are unhappy with how we have used your data.

The ICO’s address:

Information Commissioner’s Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Helpline number: 0303 123 1113

ICO website: <https://www.ico.org.uk>

# Important definitions

‘We’ means Clyde Scouts

‘ICO’ is the Information Commissioner’s Office, the body responsible for enforcing data protection legislation within the UK and the regulator authority for the purposes of GDPR

‘Local Scouting’ and ‘Scout Unit’ mean Scout Groups and Districts within the Clyde Region

‘Personal Data’ is information that relates to an identified or identifiable individual, directly from the information in question; or who can be indirectly identified from that information in combination with other information.

‘Processing’ means all aspects of handling personal data, including but not limited to collecting; storing; sharing and archiving.

‘Data Controller’ are the main decision-makers who have overall control over the purposes and means of the processing of personal data.

‘Data Processor’ act on behalf of, and only on the instructions of, the relevant controller.

‘Subject Access Request’ is a request for personal data that an organisation may hold about an individual. This request can advise to delete, provide, amend or restrict their own, the individual’s, personal data.

‘Compass’ Compass is the Scout Association’s membership system.

‘Online identifiers’ includes IP addresses and cookie identifiers which may be personal data.

# What is personal data?

As above, Personal data is information that relates to an identified or identifiable individual. Personal data only includes information relating to natural persons who:

* + can be identified or who are identifiable, directly from the information in question; or
	+ who can be indirectly identified from that information in combination with other information.

Personal data may also include special categories of personal data or criminal conviction and offences data. These are considered to be more sensitive and can only be processed in more limited circumstances. These include, but are not limited to, sexual orientation, race, political opinions and religious beliefs. Pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data. Information about a deceased person does not constitute personal data and therefore is not subject to the UK GDPR.

What are identifiers and related factors?

An individual is ‘identified’ or ‘identifiable’ if you can distinguish them from other individuals. A name is perhaps the most common means of identifying someone. However, whether any potential identifier actually identifies an individual depends on the context. A combination of identifiers may be needed to identify an individual.

The UK GDPR provides a non-exhaustive list of identifiers, including: name; identification number; location data; and an online identifier. Other factors can identify an individual.

# Data Protection and Scouting

Data protection legislation applies to all data controllers regardless of whether they are charities or small organisations. It applies to local Scouting in the same way as it does to other organisations. Scout units are created and run as independent charities and insofar as they collect and store personal data about members and young people, for example, they are data controllers and must adhere to the law.

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

* Maintenance of local Scouting’s primary records, such as name, address and leadership details of the local Group, District and Region
* Local Scouting roles, such as creation, management and deletion of role and any reasons for leaving local Scouting. This includes ID checking
* Direct messaging in the platform
* Training updates and Personal Learning Plans

As a Scout Region within Scouts Scotland and The Scout Association, our policy adheres to theirs.

# What type of personal data we collect and why?

### 6.1 Members and volunteers

We benefit from the service of a large number of members giving their time to Scouting at both Regional and local Scouting levels. We hold personal data (including special category data) about members and volunteers on the membership database, Compass. We believe it is important to be open and transparent about how we will use your personal data. Information we hold about you may include the following:

* name and contact details
* length and periods of service (and absence from service)
* details of training you receive
* details of your experience, qualifications, occupation, skills and any awards you have received
* details of Scouting events and activities you have taken part in
* details of next of kin
* age/date of birth
* details of any health conditions
* details of disclosure checks
* any complaints we have received about the member
* details about your role(s) in Scouting
* details about your membership status
* race or ethnic background and native languages
* religion
* nationality

We need this information to communicate with you and to carry out any necessary checks to make sure that you can work with young people. We also have a responsibility to keep information about you, both during your membership and afterwards (due to our safeguarding responsibilities and also to help us if you leave or re-join).

Much of this information is collected from the member joining forms

### 6.2 Trustees and members of the governance structure

For the members of The Scout Association’s Board of Trustees and its subcommittees, other committees and working groups, we may hold the type of information as set out in 6.1 and also including the following:

* CVs
* Related party information

### 6.3 Donors

We benefit from donations from members of the public who support our work, and we hold personal data about these donors so that we can process donations and tell donors about our work and campaigns and how they can support us further. We may hold the type of information as set out in 6.1.

### 6.4 Customers and visitors

We also hold personal data from customers and visitors to our Glasgow Scout Shop, Auchengillan Outdoor Centre, meetings and our other sites. We may hold the type of information as set out in 6.1 and also including the following:

* purchase history
* taxpayer and payment details

Much of this information is taken from online registration forms or our online shop.

### 6.5 Employees (past, present and future)

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

We also hold information that allows us to pay salaries and work with other payroll and pension providers. Information we may hold about staff includes the following:

* name and contact details
* length and periods of service (and absence from service)
* details of training you receive
* details of your experience, qualifications, occupation, skills
* details of next of kin
* age/date of birth
* details of any health conditions
* details of disclosure checks if applicable
* details of any dependents
* information that allows us to pay salaries and work with other payroll and pension providers
* references, and records relating to the time they worked for TSA,
* probationary, appraisal and disciplinary information.

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

### 6.6 CCTV

Our premises at Elmbank St and Auchengillan Outdoor Centre operate a CCTV network to help prevent and detect crime and safeguard (protect) young people and others. If we can identify somebody from a CCTV image, the image must be processed as personal data.

# The Law

To make sure that we are processing and holding information within the law, we must make sure that information is:

* processed fairly and lawfully
* collected for specified, clear and legitimate purposes
* adequate, relevant and limited to what is necessary
* accurate and, where necessary, kept up to date
* kept for no longer than is necessary
* processed securely

The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one of the following must apply whenever you process personal data:

* **Consent** - you have to give (or have given) your permission for us to use your information for one or more specific purposes
* **Performance of a contract** - we need to process the information to meet the terms of any contract you have entered into (for example when we process personal data as part of a volunteer’s membership application or to provide goods or services purchased with us)
* **Legal obligation** - processing the information is necessary to keep to our legal obligations as data controller
* **Vital interests** - processing the information is necessary to protect your vital interests
* **Public task** - processing the information is necessary for tasks in the public interest or for us as the data controller to carry out our responsibilities
* **Legitimate interest -** processing the information is necessary for our legitimate interests (see below examples)

|  |  |
| --- | --- |
| Lawful basis | Data processing examples |
| Consent | ·       Sending marketing information not deemed part of legitimate interest·       The use of photography captured by the Region·       Managing grant applications and provisions·       Keeping in contact after a donation or request  |
| Performance of a contract | ·       Volunteers membership application·       Supply of goods or services purchased |
| Legal obligation | ·       Responding to information requests from statutory authorities·       Disclosure and Barring Service referral·       Insurance underwriting referrals |
| Vital interests | ·       Medical history disclosure to a medical professional to protect the vital interests of the data subject |
| Legitimate interest | ·       Photography at Regional organised events where consent is not appropriate·       The passing of personal data to local Scout Groups as part of the ‘Find a local group’ service online.·       Displaying the contact details of local leaders as part of the ‘Find a local group’ service online·       Nominations for top awards (Meritorious & Gallantry, Silver Acorn, Silver Wolf) including citations·       Informational/operational communications directly to volunteers·       The use of membership data for the recruitment of Regional roles·       The passing of volunteer and young person data to TSA’s outside legal counsel in defence of cases |

### Sharing information

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

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

Some of these organisations may process information in countries outside the EEA, such as the United States, where data protection laws are not the same as in the EEA. Clyde Regional Scout Council will always ensure any transfer is subject to appropriate security measures to safeguard your personal data. Where transfers are necessary to countries where data protection has not yet been declared to be adequate, we rely on appropriate safeguards, as defined in the GDPR.

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

* We have a clear lawful basis to do so.
* If we have to supply information to others (for example payroll providers) for processing on our behalf. We do this if we are asked and to make sure that they are keeping to the GDPR and have appropriate confidentiality and security measures in place.
* For safeguarding young people or for other legal reasons.

A list of the most common third parties we share personal data with can be found below:

|  |  |  |
| --- | --- | --- |
| **3rd Party** | **Data Category** | **Purpose** |
| Compass | Personal and Special | Volunteer information database |
| Mailchimp | Personal and Special | Surveys, newsletters, member updates and purchasing confirmations  |
| Smartsheet | Personal and Special | Staff information, volunteer information and event information  |
| Disclosure Scotland | Personal and Special | Criminal records checks  |
| Cinolla | Personal and Special | Auchengillan Outdoor Centre & Pinkston commercial platform  |
| Flexibook | Personal and Special | Auchengillan Outdoor Centre & Pinkston commercial platform  |
| Sage50 | Personal and Special | Supplier details, customer details and accounts information  |
| Xero | Personal and Special | Supplier details, customer details and accounts information  |
| Statutory Authorities | Personal and Special | Statutory information requests/transfers |
| Police | Personal and Special | Police information requests |
| Microsoft | Personal and Special | Provision of core data repositories: Outlook, teams, sharepoint and one drive |
| Citruslime | Personal and Special | Glasgow Scout Shop commercial platform  |

# Keeping data secure

Everyone who handles personal data must make sure it is held securely to protect against unlawful or unauthorised processing and accidental loss or damage. Clyde Scouts make sure that we take appropriate steps to ensure that all personal data is secure and all staff/volunteers have read and understood this. Most staff and volunteers must complete the Scout GDPR training module upon starting their role. In most cases, personal data must be stored in appropriate systems and encrypted when taken off-site. The following is general guidance for everyone working within Scouting, including staff, members and volunteers in local Scouting.

* You must only store personal data on networks, drives or files that are password protected and regularly backed up.
* You should have proper entry-control systems in place, and you should report any stranger seen in entry-controlled areas.
* You should keep paper records containing personal data secure. If you need to move paper records, you should do this strictly in line with data protection rules and procedures.
* You should not download personal data to mobile devices such as laptops and USB sticks unless necessary. Access to this information must be password protected and the information should be deleted immediately after use.
* You must keep all personal data secure when travelling.
* Personal data relating to members and volunteers should usually only be stored on the membership database or other specific databases which have appropriate security in place.
* When sending larger amounts of personal data by post, you should use registered mail or a courier. Memory sticks should be encrypted.
* When sending personal data by email this must be appropriately authenticated and password protected.
* Do not send financial or sensitive information by email unless it is encrypted.
* You should not share your passwords with anyone.
* Different rights of access should be allocated to users depending on their need to access personal or confidential information. You should not have access to personal or confidential information unless you need it to carry out your role.
* Before sharing personal data with other people or organisations, you must ensure that they are GDPR compliant.
* In the event that you detect or suspect a data breach, you should follow your defined breach response process.

# Responsibilities

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

### 9. 1 Board of Trustees

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

### 9.2 Chief Operating Officer

The Chief Operating Officer is responsible for:

* making sure that this data protection policy is up to date
* advice on data protection issues
* dealing with complaints about how we use personal and sensitive personal data
* reporting to the ICO if we do not keep to any regulations or legislation

### 9.3 Staff

All staff have a responsibility to keep to the requirements of this data protection policy and our related procedures and processes. Managers are responsible for making sure that staff within their teams are aware of and keep to this. If you become aware of a data protection issue you must report it promptly to the Chief Operating Officer, or Board of Trustees in their absence.

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

### Volunteers, members and local Scouting

We expect volunteers to keep to data protection legislation and this data protection policy, and to follow the relevant rules set out in our Policy, Organisation and Rules (POR). The local Executive Committee (trustees of local Groups & Districts) has overall responsibility for keeping to data protection regulations.

# Data Retention

We may keep information for different periods of time for different purposes as required by law or best practice. Individual departments include these time periods in their processes. We make sure we store this in line with our archiving policy, as follows:

1. Application forms – for period of employment (voluntary or paid)
2. References – 1 year from date of receipt
3. Payroll and tax information – 10 years
4. Sickness records – 5 years
5. Annual Leave records – 5 years
6. Special leave records – 5 years
7. Appraisals – 5years
8. Promotions/Transfers/Disciplinary – 1 year from end of employment
9. Training – 1 year from end of employment
10. Injury or accident at work – 12 years from end of employment
11. Enquiry information – 2 years from when it has been actioned
12. Cookies – browsing information is stored by our website domain please read cookie information.

As far as membership information is concerned, to make sure of continuity (for example if you leave and then re-join) and to carry out our legal responsibilities relating to safeguarding young people, we keep your membership information throughout your membership and after it ends, and we make sure we store it securely. Only those staff who need membership information to carry out their role have access to that information.

# Subject Access Request

The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data, as well as other supplementary information.

### 11.1 How do we recognise a subject access request (SAR)?

An individual can make a SAR verbally or in writing, including on social media. A request is valid if it is clear that the individual is asking for their own personal data. An individual does not need to use a specific form of words, refer to legislation or direct the request to a specific contact.

An individual may ask a third party (eg a relative, friend or solicitor) to make a SAR on their behalf. You may also receive a SAR made on behalf of an individual through an online portal. It is the third party’s responsibility to provide evidence of their authority.

### 11.2 What about requests for information about children?

Before responding to a SAR for information held about a child, we will consider whether the child is mature enough to understand their rights. If the request is from a child and we are confident they can understand their rights, we will usually respond directly to the child. We may, however, allow the parent or guardian to exercise the child’s rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child. If a child is competent, they may authorise someone else, other than a parent or guardian, to make a SAR on their behalf.

### 11.3 What should we consider when responding to a request?

It is a legal requirement to comply with a SAR without undue delay and at the latest within one month of receiving the request. We can extend the time to respond by a further two months if the request is complex or we have received a number of requests from the individual, eg other types of requests relating to individuals’ rights.

If further clarification is required, such as identification, for the request, the time limit for responding to the request is paused until clarification is received.

### 11.4 Accessing and updating

Under data protection law, individuals have more than just the right to access their personal data. These include:
a. Rectify – the right to correct any mistakes
b. Erase – the right to request we destroy any personal data and/or withdraw consent
c. Restrict processing – where, for lawful or legitimate purposes we cannot destroy relevant personal data, we can store it for restricted purposes
d. Notify third parties – the right to advise us to notify third parties of the request for access or any of the above.
e. Object – the right to object to the processing of personal information