**8th Darlington (Cockerton Green) Scout Group – Data Protection Policy**

Date: 6 August 2024
Prepared by: Liam Pape
Reviewed by: Executive Leadership Team

**Introduction**

**The 8th Darlington (Cockerton Green) Scout Group** ("We" in this document) is a data controller and directly responsible for any personal data we process and must ensure we are aware of their responsibilities under the law.

**1. Purpose of this Data Protection policy and what it covers**
This policy sets out the 8th Darlington (Cockerton Green) Scout Group's approach to protecting personal data. We are registered with the Information Commissioner's Office at the following address: 80-82 Cockerton Green, Darlington DL3 9EU. If you have any queries about anything set out in this policy or about your own rights, please contact us at scouts8thdarlington@outlook.com

**2. Some Important Definitions**
**'We'** means The 8th Darlington (Cockerton Green) Scout Group

**'ICO'** is the Information Commissioner's Office, the body responsible for enforcing data protection legislation within the UK and the regulatory authority for the purposes of the GDPR

**'Processing'** means all aspects of handling personal data, for example collecting, recording, keeping, storing, sharing, archiving, deleting and destroying it.

**'Data Controller'** means anyone (a person, people, public authority, agency or any other body) which, on its own or with others, decides the purposes and methods of processing personal data. We are a data controller insofar as we process personal data in the ways described in this policy.

**'Data processor'** means anyone who processes personal data under the data controller's instructions, for example a service provider. We act as a data processor in certain circumstances.

**'Subject Access Request'** is a request for personal data that an organisation may hold about an individual. This request can be extended to include the deletion, rectification and restriction of processing.

**3. What is personal data?**

Personal data includes any information that can identify a person, such as home addresses, phone numbers, email addresses, and occupation. Special category data, which is particularly sensitive, includes racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic and biometric data, and information about sex life or sexual orientation.

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

We hold personal data (including special category data) about adult and child members and volunteers on our membership database. We believe it is important to be open and transparent

about how we will use your personal data. Information we hold about you may include the following:

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

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

For Young People, in addition to the above, we may also hold information, we may hold information where there has been a safeguarding case raised, this may include basic personal identifiers along with the details of the case.

**5.3 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. This may include details of donors that wish to leave a legacy in their Will.

We may hold the following type of information:

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

**5.4 Customers and visitors**

We also hold personal data for visitors to our sites. This can include guests, suppliers, tradespeople and contractors. Much of this information is taken from online registration forms and emails.

**5.5 CCTV**

Our Headquarters operates a CCTV network to help prevent and detect crime and protect young people and others. If we can identify somebody from a CCTV image, the image must be processed as personal data.

**6. Conditions for collecting personal data**
**6.1 Keeping to the law**

We must keep to the law when processing personal data. To achieve this, we have to meet at least one of the following conditions:

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

| Lawful basis | Data processing examples |
|---|---|
| Consent | • Sending marketing information not deemed part of legitimate interest. |
| Performance of a contract | • Supply of goods or services purchased. |
| Legal obligation | • Responding to information requests from statutory authorities.<br>• Disclosure and Barring Service referral.<br>• Insurance underwriting referrals. |
| Vital interests | • Medical history disclosure to a medical professional to protect the vital interests of the data subject. |
| Public task | • Sharing information with statutory bodies such as the Police (including the Hydrant Programme) or Local Authorities. |
| Legitimate interest | • Photography at organised events where consent is not appropriate (could include the publishing of the photography in social media and printed format).<br>• Informational/operational communications directly to volunteers.<br>• The use of membership data for the recruitment of Exeuctive Leadership Team roles. |

Also, information must be:

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

**6.2 Information that we share**

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

- We have a clear lawful basis to do so.
- If we have to supply information to others 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.

**7. Keeping personal data secure**

Everyone who handles personal data (including staff, members, volunteers, payroll and pension providers) must make sure it is held securely to protect against unlawful or unauthorised processing and accidental loss or damage. We take appropriate steps to make sure we keep all personal data secure, and we make all of our adult members aware of these steps. 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 the Group, including staff, members and volunteers:

- 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.

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

**8.1 Executive Leadership Committee**

Our Executive Leadership Committee has overall responsibility for making sure that we keep to legal requirements, including data protection legislation.

**8.2 Volunteers and members**

We expect you to keep to data protection legislation and this data protection policy, and to follow the relevant rules set out in our Policy, Organisation and Rules (POR).

The local Executive Committee (trustees of local Groups, Districts, Areas, Counties, Countries and so on) has overall responsibility for keeping to data protection regulations.

As part of your data protection duties, you should report urgently (to the Executive Leadership Committee) any instance where the rules on how we handle personal data are broken (or might be broken).

**9. Data Retention**
We may keep information for different periods of time for different purposes as required by law or best practice. Individual departments include these time periods in their processes.

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

Only those staff who need membership information to carry out their role have access to that information.

**10. Rights to accessing and updating personal data**
Under data protection law, individuals have a number of rights in relation to their personal data.

a. The right to information: As a data controller, we must give you a certain amount of information about how we collect and process information about you. This information needs to be concise, transparent, understandable and accessible.
b. The right of subject access: If you want a copy of the personal data we hold about you, you have the right to make a subject access request (SAR) and get a copy of that information within 30 days.
c. The right to rectification: You have the right to ask us, as data controller, to correct mistakes in the personal data we hold about you.

d. The right to erasure (right to be forgotten): You can ask us to delete your personal data if it is no longer needed for its original purpose, or if you have given us permission to process it and you withdraw that permission (or where there is no other lawful basis for processing it).
e. The right to restrict processing: In certain circumstances where, for lawful or legitimate purposes we cannot delete your relevant personal information or if you do not want us to delete it, we can continue to store it for restricted purposes. This is an absolute right unless we have a lawful purpose to have it that overwrites your rights.
f. The obligation to notify relevant third parties: If we have shared information with other people or organisations, and you then ask us to do either (c), (d) or (e) above, as data controller we must tell the other person or organisation (unless this is impossible or involves effort that is out of proportion to the matter).
g. The right to data portability: This allows you to transfer your personal data from one data controller to another.
h. The right to object: You have a right to object to us processing your personal data for certain reasons, as well as the right to object to processing carried out for profiling or direct marketing.
i. The right to not be evaluated on the basis of automatic processing: You have the right not to be affected by decisions based only on automated processing which may significantly affect you.
j. The right to bring class actions: You have the right to be collectively represented by not-for-profit organisations.

**11. Subject access requests**

You are entitled to ask us, in writing, for a copy of the personal data we hold about you. This is known as a subject access request (SAR). In line with legislation, we will not charge a fee for this information and will respond to your request within one calendar month, though if the request is deemed to be complex we may take up to three months. If the request is deemed excessive, we will contact you within the month of making the SAR to state the reason and discuss how we will proceed which may include making a charge.

**Subject access requests**

Subject access requests for data held by 8th Darlington (Cockerton Green) Scout Group should be made to scouts8thdarlington@outlook.com or by writing to:

8th Darlington (Cockerton Green) Scout Group
80-82 Cockerton Green
Darlington
DL3 9EU

In situations where you feel The 8th Darlington (Cockerton Green) Scout Group has not handled your personal data query/complaint appropriately you have the right to inform the Information Commissioners Office, though you may contact them at any time.