



SENIOR VOLUNTEER NETWORK

Data Protection Policy

March 2018

Senior Volunteer Network is committed to protecting all information that we handle about people we support and work with, and to respecting people’s rights around how their information is handled. This policy explains our responsibilities and how we will meet them.

Contents

1.	Policy statement	3
2.	Why this policy is important	3
3.	How this policy applies to you and what you need to know.....	3
	<u>Section B – Our data protection responsibilities</u>	4
4.	What personal information do we process?	4
5.	Making sure processing is fair and lawful	4
6.	When we need consent to process data	5
7.	Processing for specified purposes.....	5
8.	Data will be adequate, relevant and not excessive	5
	Accurate data	6
9.	Keeping data and destroying it.....	6
10.	Security of personal data.....	6
11.	Keeping records of our data processing.....	6
	<u>Section C – Working with people we process data about (data subjects)</u>	6
12.	Data subjects’ rights	6
	<u>Schedule 1 – Definitions and useful terms</u>	8

Section A – What this policy is for

1. Policy statement

- 1.1 Senior Volunteer network is committed to protecting personal data and respecting the rights of the people whose **personal data** we collect and use. We value the personal information entrusted to us and we respect that trust, by complying with all relevant laws, and adopting good practice.

We process personal data to help us:

- a) maintain our list of SVN members and project volunteers
- b) recruit, support and manage volunteers and projects
- c) maintain our accounts and records;

This policy has been approved by the SVN Charity Trustees who are responsible for ensuring that we comply with all our legal obligations. It sets out the legal rules that apply whenever we obtain, store or use personal data.

2. Why this policy is important

- 2.1 We are committed to protecting personal data from being misused, getting into the wrong hands as a result of poor security or being shared carelessly, or being inaccurate, as we are aware that people can be upset or harmed if any of these things happen.
- 2.2 This policy sets out the measures we are committed to taking as an organisation and, what each of us will do to ensure we comply with the relevant legislation.
- 2.3 In particular, we will make sure that all personal data is:
- a) processed **lawfully, fairly and in a transparent manner**;
 - b) processed for **specified, explicit and legitimate purposes** and not in a manner that is incompatible with those purposes;
 - c) **adequate, relevant and limited to what is necessary** for the purposes for which it is being processed;
 - d) **accurate** and, where necessary, up to date;
 - e) **not kept longer than necessary** for the purposes for which it is being processed;
 - f) processed in a **secure** manner, by using appropriate technical and organisational means;
 - g) processed in keeping with the **rights of data subjects** regarding their personal data.

3. How this policy applies to you & what you need to know

- 3.1 **As trustee or volunteer** processing personal information on behalf of SVN you are required to comply with this policy. If you think that you have accidentally breached the

policy it is important that you contact our Data Protection Officer immediately so that we can take swift action to try and limit the impact of the breach.

Anyone who breaches the Data Protection Policy may be subject to disciplinary action, and where that individual has breached the policy intentionally, recklessly, or for personal benefit they may also be liable to prosecution or to regulatory action.

- 3.2 **As a Trustee/leader** : You are required to make sure that any procedures that involve personal data follow the rules set out in this Data Protection Policy.
- 3.3 **As a data subject of SVN** We will handle your personal information in line with this policy.
- 3.4 **Our Data Protection Officer** is responsible for advising SVN about their legal obligations under data protection law, monitoring compliance with data protection law, dealing with data security breaches and with the development of this policy. Any questions about this policy or any concerns that the policy has not been followed should be referred to them at svnetprojects@gmail.com
- 3.5 Before you collect or handle any personal data as part of your work (paid or otherwise) for SVN it is important that you take the time to read this policy carefully and understand what is required of you, as well as the organisation's responsibilities when we process data.
- 3.6 Our procedures will be in line with the requirements of this policy, but if you are unsure about whether anything you plan to do, or are currently doing, might breach this policy you must first speak to the Data Protection Officer

Section B – Our data protection responsibilities

4. What personal information do we process?

- 4.1 In the course of the work of SVN, we will collect and process information (personal data) from our members (data subjects). This is data we receive straight from the person it is about, for example, where they complete forms or contact us. Data may also be received via the website contact form.
- 4.2 We process personal data in both electronic and paper form and all this data is protected under data protection law. The personal data we process can include information such as names and contact details, education or employment details, projects completed and roles held (if appropriate), debriefing notes and visual images of people on the website.

5. Making sure processing is fair and lawful

- 5.1 Processing of personal data will only be fair and lawful when the purpose for the processing meets a legal basis, as listed below, and when the processing is transparent. This means we will provide people with an explanation of how and why we process their

personal data at the point we collect data from them, as well as when we collect data about them from other sources.

How can we legally use personal data?

- 5.2 We can lawfully use personal data according to Article 6 of the General Data Protection Regulation, for the following reasons:
- a) the processing is **necessary for legitimate interests** pursued by SVN unless these are overridden by the interests, rights and freedoms of the data subject.
 - b) we may also need to process data to comply with any legal obligation
 - c) If none of the other legal conditions apply, the processing will only be lawful if the data subject has given their clear **consent**.
- 5.3 We will only process special categories of your personal data such as medical data in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting the Data Protection Officer.

What must we tell individuals before we use their data?

- 5.4. Information concerning our legitimate interests for collecting and using personal data, how the data will be stored and for how long the data will be kept will be in the **Privacy notice** which will accompany any request for personal data. This notice will also appear on the website where SVN may be contacted.

If we plan to pass the data onto someone else outside of SVN we will give the data subject this information before we pass on the data.

6. When we need consent to process data

- 6.1 Where none of the other legal conditions apply to the processing, and we are required to get consent from the data subject, we will clearly set out what we are asking consent for, including why we are collecting the data and how we plan to use it. Consent will be specific to each process we are requesting consent for and we will only ask for consent when the data subject has a real choice whether or not to provide us with their data.
- 6.2 Consent can however be withdrawn at any time and if withdrawn, the processing will stop. Data subjects will be informed of their right to withdraw consent and it will be as easy to withdraw consent as it is to give consent.

7. Processing for specified purposes

- 7.1 We will only process personal data for the specific purposes explained in our privacy notice, or for other purposes specifically permitted by law.

8. Data will be adequate, relevant and not excessive

- 8.1 We will only collect and use personal data that is needed for the specific purposes described above (which will normally be explained to the data subjects in privacy notices). We will not collect more than is needed to achieve those purposes. We will not collect any personal data “just in case” we want to process it later.

Accurate data

- 8.2 We will make sure that personal data held is accurate and, where appropriate, kept up to date. The accuracy of personal data will be checked at the point of collection and at appropriate points later on.

9. Keeping data and destroying it

- 9.1 We will not keep personal data longer than is necessary for the purposes that it was collected for. Data will normally be removed from the data base when the subject is no longer a member of SVN. Lists of names with projects completed may be kept for archival purposes as explained in the Privacy Notice. Personal Data will be reviewed every 5 years

10. Security of personal data

- 10.1 We will use appropriate measures to keep personal data secure at all points of the processing. Keeping data secure includes protecting it from unauthorised or unlawful processing, or from accidental loss, destruction or damage.
- 10.2 We will implement security measures which provide a level of security which is appropriate to the risks involved in the processing. This includes technical and organisational measures.
- 10.3 In assessing what measures are the most appropriate we will take into account the following: quality, cost of security measure, nature and scope of processing data, risk to freedoms and rights of the data subject, risks which could result from a data breach, and anything else that is relevant

Such measures may include those to restrict or minimise access to data, measures to ensure systems and data remain available and can be easily restored in the event of an incident.

11. Keeping records of our data processing

- 11.1 To show how we comply with the law we will keep clear records of our processing activities and of the decisions we make concerning personal data (setting out our reasons for those decisions).
- 11.2 Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result

in a risk to the rights and freedoms of individuals then we must also notify the Information Commissioner's Office within 72 hours.

If you are aware of a data breach you must contact The Data Protection Officer immediately and keep any evidence you have in relation to the breach.

Section C – Working with people we process data about (data subjects)

12. Data subjects' rights

12.1 We will process personal data in line with data subjects' rights, including their right to:

- a) request access to any of their personal data held by us. Data subjects can make a '**subject access request**' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request you should forward it immediately to the Data Protection Officer who will coordinate a response.
- b) ask to have inaccurate personal data changed;
- c) restrict processing, in certain circumstances;
- d) object to processing, in certain circumstances.
- e) data portability, which means to receive their data, or some of their data, in a format that can be easily used by another person (including the data subject themselves) or organisation;
- f) withdraw consent when we are relying on consent to process their data.

12.2 If a member of the leadership team receives any request from a data subject that relates or could relate to their data protection rights, this will be forwarded to our Data Protection Officer **immediately**.

12.3 We will act on all valid requests as soon as possible, and at the latest within **one calendar month**, unless we have reason to, and can lawfully extend the timescale. This can be extended by up to two months in some circumstances.

12.4 All data subjects' rights are provided free of charge.

12.5 Any information provided to data subjects will be concise and transparent, using clear and plain language.

Schedule 1 – Definitions and useful terms

The following terms are used throughout this policy and have their legal meaning as set out within the General Data Protection Regulation. The GDPR definitions are further explained below:

Data controller means any person, company, authority or other body who (or which) determines the means for processing personal data and the purposes for which it is processed. It does not matter if the decisions are made alone or jointly with others.

The data controller is responsible for the personal data which is processed and the way in which it is processed. We are the data controller of data which we process.

Data processors include any individuals or organisations, which process personal data on our behalf and on our instructions e.g. an external organisation which provides secure waste disposal for us. This definition will include the data processors' own staff (note that staff of data processors may also be data subjects).

Data subjects include all living individuals who we hold or otherwise process personal data about. A data subject does not need to be a UK national or resident. All data subjects have legal rights in relation to their personal information. Data subjects that we are likely to hold personal data about include:

- a) the people we care for and support;
- b) our employees (and former employees);
- c) consultants/individuals who are our contractors or employees working for them;
- d) volunteers;
- e) tenants;
- f) trustees;
- g) complainants;
- h) supporters;
- i) enquirers;
- j) friends and family;
- k) advisers and representatives of other organisations.

ICO means the Information Commissioners Office which is the UK's regulatory body responsible for ensuring that we comply with our legal data protection duties. The ICO produces guidance on how to implement data protection law and can take regulatory action where a breach occurs.

Personal data means any information relating to a natural person (living person) who is either identified or is identifiable. A natural person must be an individual and cannot be a company or a public body. Representatives of companies or public bodies would, however, be natural persons.

Personal data is limited to information about living individuals and does not cover deceased people.

Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

Privacy notice means the information given to data subjects which explains how we process their data and for what purposes.

Processing is very widely defined and includes any activity that involves the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing can also include transferring personal data to third parties, listening to a recorded message (e.g. on voicemail) or viewing personal data on a screen or in a paper document which forms part of a structured filing system. Viewing of clear, moving or stills images of living individuals is also a processing activity.

Special categories of data (as identified in the GDPR) includes information about a person's:

- l) Racial or ethnic origin;
- m) Political opinions;
- n) Religious or similar (e.g. philosophical) beliefs;
- o) Trade union membership;
- p) Health (including physical and mental health, and the provision of health care services);
- q) Genetic data;
- r) Biometric data;
- s) Sexual life and sexual orientation.