Data Protection Policy

Background

SERVE ON is committed to being transparent about how we collect and use the personal data of our volunteers, employees, contractors and stakeholders and to meeting our obligations described in the Data Protection Act. This policy sets out our commitment to data protection, and individual rights and obligations in relation to personal data. The purpose of this policy is to ensure that all personal data held by us is processed lawfully, fairly, and transparently, and that the rights of data subjects are protected.

This policy applies to all personal data collected including that of job applicants, employees, contractors, volunteers, former employees, trustees and advisors.

Terminology/ interpretation

Personal data: is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

Special categories of personal data: means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data.

Criminal records data: means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Trustees/ Board members: Trustees/ Board members are the people who are responsible for the general control of the management of the administration of our organisation.

Data protection responsibility

SERVE ON has appointed Abb Dhanani as the person with responsibility for data protection compliance within the organisation. Questions about this policy, or requests for further information, should be directed to him. The SERVE ON Board has overall accountability for ensuring data protection compliance.

Data protection principles

SERVE ON processes personal data in accordance with the following data protection principles. We:

- process personal data lawfully, fairly and in a transparent manner
- collect personal data only for specified, explicit and legitimate purposes
- process personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing
- keep accurate personal data and take all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay
- keep personal data only for the period necessary for processing
- adopt appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, accidental loss, destruction or damage

SERVE ON tells individuals the reasons for processing their personal data, how we use such data and the legal basis for processing in our privacy notices. It will not process personal data of individuals for other reasons. If SERVE ON wants to start processing personal data for other reasons, individuals will be informed of this before any processing begins and will be given the opportunity to opt out.

Identifiable personal data will not be shared with third parties. If SERVE ON wish to change this in the future, we will inform individuals and, where we rely on legitimate interests as the basis for processing data, we will carry out an assessment to ensure that those interests are not overridden by the rights and

freedoms of individuals. Supporters will not receive mailshots from SERVE ON outside of updates of our work. If we want to change this, we will consult first.

Should we need to process special categories of personal data or criminal records data to perform obligations, to exercise rights in employment law, or for reasons of substantial public interest, it will be done in accordance with a policy on processing special categories of data and criminal records data.

We will update personal data promptly if an individual advises that their information has changed or is inaccurate.

Personal data gathered will be securely held and access to that information will be limited to the Leadership Team and specific individuals who have administrative roles that require access. For example, passport details, Next-of-Kin info and medical information will be recorded for IRT members to facilitate rapid, safe deployment.

The period for which the organisation holds personal data will be in line with legislation. Personal information of members who have left the organisation will be erased within 9 months of them leaving.

Individual rights

As a data subject, individuals have rights in relation to their personal data.

We do not have plans to share this data with third parties for unspecified reasons. For complete transparency, we would share info for specific reasons that directly relate to our charitable work, for example, we would share passport details with an organisation that is involved in booking flights for the IRT so that they can deploy abroad in an emergency.

Individuals have the right to make a subject access request. If an individual makes a subject access request, we will tell them:

- whether their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual
-

- to whom their data is or may be disclosed, including to recipients located outside the UK and the safeguards that apply to such transfers
- for how long their personal data is stored (or how that period is decided)
- their rights to rectification or erasure of data, or to restrict or object to processing
- their right to complain to the Information Commissioner's Office if they think we have failed to comply with our data protection rights
- whether we carry out automated decision-making and the logic involved in any such decision-making

We will also provide the individual with an electronic copy of the personal data undergoing processing.

Other rights

Individuals have other rights in relation to their personal data. They can require the organisation to:

- rectify inaccurate data
- stop processing or erase data that is no longer necessary for the purposes of processing
- stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data)
- stop processing or erase data if processing is unlawful

Data security

We take the security of personal data seriously. We have taken steps to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed other than for legitimate means. We do this by limiting access and securely storing the information on Google Drive. Google

Drive is secure in that it employs industry-standard measures like AES 256-bit encryption for data in transit and at rest, secure Google data centers, and built-in threat detection to block spam, phishing, and malware.

Data breaches

If SERVE ON discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, we will report it to the Information Commissioner within 72 hours of discovery. We will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, we will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

Individual responsibilities

Individuals are responsible for helping SERVE ON keep their personal data up to date. Individuals should let SERVE ON know if data provided to the organisation changes, for example if an individual changes their phone number or their Next-of-Kin details change.

Trustees, employees and contractors may have access to the personal data of other individuals in the course of their duties. Where this is the case, we rely on individuals to help meet our data protection obligations.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes
- not to disclose data except to individuals inside the organisation who have appropriate responsibility
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction

- not to remove personal data, or devices containing or that can be used to access personal data, from the SERVE ON's systems without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device
- not to store personal data on local drives or on personal devices that are used for work purposes
- to immediately report data breaches of which they become aware, to the Board

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under our disciplinary procedure if it applies to you. Significant or deliberate breaches of this policy, such as accessing employee or volunteer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice

Version Control

Please note that this version control is for Serve On use only. This section details the changes made to the documents and does not reference any individual's circumstances.

Version Number	Date	Revision Author	Description
1	14.10.2025	Elle Hallaway	Initial version with retention period

Accountable person

Person accountable for this policy	Role	Organisation
	Trustees	Serve On

Document Review

Date of Policy Review	Policy reviewed by	Date of next Policy Review	Policy to be reviewed by
01.09.2026	Board	01.09.2026	Board