SANHS
Data Protection Policy

Table of Contents

Adopted by SANHS Board on 5th November 2018
Next review December 2019

INTRODUCTION

SANHS is committed to protecting the rights and freedoms of its data subjects and safely and securely processing their data in accordance with all its legal obligations. The Society holds personal data about its members and other individuals for a variety of charitable purposes. This policy sets out how SANHS seeks to protect personal data and ensure that its members, volunteers and the Office Manager understand the rules governing the use of personal data to which they have access during their work.

This policy requires data processors to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed. This policy has been written to ensure compliance with the Data Protection Act 2018 which enshrines in UK law the EU General Data Protection Regulations.

DEFINITIONS

Business purposes	The purposes for which personal data may be used by SANHS can be categorised as personnel, administrative, financial, regulatory, payroll and business development purposes. Business purposes include the following: • Compliance with legal, regulatory and corporate governance obligations and good practice. • Operational reasons, such as recording transactions, fund-raising, promoting and organising events, contact by email, investigating complaints and processing membership fees. • Checking references, ensuring safe working practices, monitoring and managing access to systems and facilities and general administration. • Marketing the charity and improving services.
Personal data	'Personal data' means any information that identifies a person. SANHS may collect the following personal information: an individual's age, address, phone number, email address, subscription details and details of education and skills. SANHS does not collect the special categories of personal data specified in the Act (See Note 1).
Data controller	Data controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing personal data; where the purposes and means of such processing are determined by law. SANHS in this Policy acts as a data controller. In SANHS, the responsibility of data controller will be vested in the board Data Protection Officer appointee.
Data processor	'Data processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. In SANHS, this will mean the Office Manager and other persons processing personal data as well as third parties processing data on behalf of SANHS.
Processing	'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration,

retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

SCOPE

This policy applies to all those submitting personal data to SANHS. SANHS may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be approved by the Board before being adopted.

Who is responsible for this policy?
The Data Protection Officer (DPO), a Board appointee, has overall responsibility for the day-to-day implementation of this policy.

PRINCIPLES

SANHS will comply with the principles of data protection (the Principles) enumerated in the EU General Data Protection Regulation. SANHS will make every effort possible in everything SANHS does to comply with these principles. The Principles are:

1. Lawful, fair and transparent
Data collection must be fair, for a legal purpose and SANHS must be open and transparent as to how the data will be used.

2. Limited for its purpose
Data can only be collected for a specific purpose.

3. Data minimisation
Any data collected must be necessary and not excessive for its purpose.

4. Accurate
The data SANHS holds must be accurate and kept up to date.

5. Retention
SANHS cannot store data longer than necessary. Personal data will be archived unless the data subject or their representative, asks the Society to delete it.

6. Integrity and confidentiality
The data SANHS holds must be kept safe and secure.

Accountability and transparency

SANHS must ensure accountability and transparency in all its use of personal data and must show how it complies with each Principle. Data Processors are responsible for keeping a written record of how all their data processing activities comply with each of the Principles. This must be kept up to date and must be approved by the DPO.

To comply with data protection laws and the accountability and transparency Principle of GDPR, SANHS must demonstrate compliance. The DPO is responsible for understanding the Society's responsibilities to ensure SANHS meet the following data protection obligations:

- Fully implement all appropriate technical and organisational measures.
- Maintain up to date and relevant documentation on all processing activities.
- Implement measures to ensure privacy by design and default, including:
    - Data minimisation
    - Pseudonymisation
    - Transparency
    - Creating and improving security and enhanced privacy procedures on an ongoing basis

Procedures

See Note 2

PERSONNEL RESPONSIBILE FOR PROCESSING PERSONAL DATA

SANHS general responsibilities

- Analyse and document the type of personal data SANHS holds.
- Check procedures to ensure they cover all the rights of the individual.
- Ensure consent procedures are lawful.
- Implement procedures to detect, report and investigate personal data breaches.
- Store data in safe and secure ways.

Data Processor responsibilities

- Check that any data processing activities comply with the Data Protection Policy and are justified.
- Use data in a lawful way.
- Store data correctly and according to the SANHS Data Protection Policy.
- Fully understand SANHS' data protection obligations.
- Comply with this policy at all times.
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or legal obligations, to the DPO without delay.
- Ensure all systems, services, software and equipment meet acceptable security standards.
- Check and scan security hardware and software regularly to ensure it is functioning properly.
- Research third-party services, such as cloud services that SANHS is considering using to store or process data.
- Approve data protection statements attached to emails and other marketing copy.
- Address data protection queries from members, volunteers, or media outlets.

- Coordinate with the DPO to ensure all marketing initiatives adhere to data protection laws and this Data Protection Policy.
- Familiarisation of regulations governing international transfers of personal data (personal data must not be transferred abroad or anywhere else outside of normal rules and procedures without express permission from the DPO).

Board Data Protection Officer responsibilities

- Keep the board updated about data protection responsibilities, risks and issues.
- Review all data protection procedures and policies on a regular basis.
- Arrange data protection training and advice for all relevant members and those included in this policy.
- Answer questions on data protection from board members and other stakeholders.
- Respond to individuals such as members and other persons who wish to know which data is being held on them.
- Check and approve with third parties that handle the SANHS data any contracts or agreement regarding data processing.

ACCURACY AND SECURITY OF PERSONAL DATA

Accuracy and relevance

SANHS will ensure that personal data that it processes is accurate, adequate, relevant, and not excessive, given the purpose for which it was obtained. Individuals can ask to correct inaccurate personal data relating to them.

Data security

SANHS must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on behalf of SANHS, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations. Existing third parties are: MailChimp; PayPal; NatWest; Carbonite; HMRC; MS Azure; Donorfy.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it.
- Printed data should be shredded when it is no longer needed.
- Data stored on a computer should be protected by passwords that are changed regularly.
- Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used.
- The DPO must approve any cloud server used to store data.
- Servers containing personal data must be kept in a secure location, away from general office space.
- Data should be regularly backed up in line with the SANHS backup procedures.

- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.
- All servers containing sensitive data must be approved and protected by security software.
- All possible technical measures must be put in place to keep data secure.

Data retention and disposal
Under GDPR, personal data cannot be retained for longer than the purpose for which it was processed. The exception to this principle is the archiving of personal data for public interest. SANHS will archive personal data unless requested to delete it by the data subject or their representative.

RIGHTS OF INDIVIDUALS
See Note 3

AUDITS AND MONITORING AND REPORTING BREACHES
See Note 4

THIRD PARTIES
See Note 5

FAILURE TO COMPLY
SANHS take compliance with this policy very seriously. Failure to comply puts SANHS and its members at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action towards a member, volunteer or the Office Manager. If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.

This policy is to be read in conjunction with the SANHS Welfare Policy.
Documentation of procedures (see Note 2) will be held in the SANHS office.

References

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
https://services.parliament.uk/bills/2017-19/dataprotection.html
https://vinciworks.com/blog/free-data-protection-privacy-policy-template

All accessed March 2018

Adopted by Board on:

Policy review due: **November 2019**

NOTES

Note 1

Special categories of personal data
What are special categories of personal data?
Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sexual orientation

In most cases where SANHS processes special categories of personal data, SANHS will require the data subject's *explicit* consent to do this unless exceptional circumstances apply or SANHS is required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed. The condition for processing special categories of personal data must comply with the law. If SANHS do not have a lawful basis for processing special categories of data that processing activity must cease.

Note 2

Procedures

Fair and lawful processing
SANHS must process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. SANHS will not process personal data unless the individual whose details SANHS are processing has consented to this happening. If SANHS cannot apply a lawful basis, its processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed erased.

Controlling data
As a data controller, SANHS must comply with its contractual obligations. In processing data, SANHS must:

- Not use a third-party without written authorisation of the DPO.

- Ensure the security of the processing.
- Keep accurate records of processing activities.

Lawful basis for processing data
SANHS must establish a lawful basis for processing data. At least one of the following conditions must apply whenever SANHS processes personal data:

- **Consent:** SANHS holds recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.
- **Contract:** The processing is necessary to fulfil or prepare a contract for the individual.
- **Public function:** Processing is necessary to carry out a public function, a task of public interest or the function has a clear basis in law.
- **Legitimate interest:** The processing is necessary for SANHS' legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

Deciding which condition to rely on
In making an assessment of the lawful basis, SANHS must first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. SANHS cannot rely on a lawful basis if SANHS can reasonably achieve the same purpose by some other means. Remember that more than one basis may apply, and SANHS should rely on what will best fit the purpose, not what is easiest. Consider the following factors and document answers:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Whom does the processing benefit?
- What is the impact of the processing on the individual?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Are you able to stop the processing at any time on request?

SANHS' commitment to the first Principle requires it to document this process and show that SANHS has considered which lawful basis best applies to each processing purpose, and fully justify these decisions. SANHS must also ensure that individuals whose data is being processed are informed of the intended purpose. This will occur via the Privacy Notice. Documentation of procedures will be held in the SANHS office and will be approved by the Board after presentation by the Data Protection Officer.

Note 3

Rights of individuals

Individuals have rights to their data which SANHS must respect and comply with to the best of its ability. SANHS must ensure individuals can exercise their rights in the following ways:

1. Right to be informed

- Supply Privacy Notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.
- Keep a record of how SANHS uses personal data to demonstrate compliance with the need for accountability and transparency.

2. Right of access

- Permit individuals to access their personal data and supplementary information.
- Allow individuals to be aware of and verify the lawfulness of the processing activities.

3. Right to rectification

- SANHS must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete. This must be done without delay, and no later than one month. This can be extended to two months with permission from the DPO.

4. Right to erasure

- SANHS must delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

5. Right to restrict processing

- SANHS must comply with any request to restrict, block, or otherwise suppress the processing of personal data.
- SANHS are permitted to store personal data if it has been restricted, but not process it further. SANHS must retain enough data to ensure the right to restriction is respected in the future.

6. Right to data portability

- SANHS must provide individuals with their data so that they can reuse it for their own purposes or across different services.
- SANHS must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

7. Right to object

- SANHS must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- SANHS must respect the right of an individual to object to direct marketing, including profiling.
- SANHS must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

8. Rights in relation to automated decision making and profiling

- SANHS must respect the rights of individuals in relation to automated decision making and profiling.
- Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

Privacy Notices

When to supply a Privacy Notice?
A Privacy Notice must be supplied at the time the data is obtained if obtained directly from the data subject. If disclosure to another recipient is envisaged, then the Privacy Notice must be supplied prior to the data being disclosed. In March 2018, all current members of SANHS were sent a Privacy Notice to sign and return. SANHS will send each new member a Privacy Notice when they join the Society and advise members of updated Privacy Notices via email and post.

What to include in a Privacy Notice?
Privacy Notices must be concise, transparent, intelligible and easily accessible. They are provided free of charge and must be written in clear and plain language, particularly if aimed at children
The following information must be included in a Privacy Notice to all data subjects:

- Identification and contact information of the data processor and the data protection officer.
- The purpose of processing the data and the lawful basis for doing so.
- The right to withdraw consent at any time, if applicable.
- The category of the personal data (only for data not obtained directly from the data subject).
- Any recipient or categories of recipients of the personal data.
- Detailed information of any transfers to third countries and safeguards in place.
- The right to lodge a complaint using internal complaint procedures.
- Any existence of automated decision making, including profiling and information about how. those decisions are made, their significances and consequences to the data subject.

Subject Access Requests

What is a Subject Access Request?
An individual has the right to receive confirmation that their data is being processed, access to their personal data and supplementary information which means the information which should be provided in a Privacy Notice.

How SANHS must deal with Subject Access Requests
SANHS must provide an individual with a copy of the information they request, free of charge. This must occur without delay, and within one month of receipt. SANHS endeavours to provide data subjects access to their information in commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system. If complying with the request is complex or numerous, the deadline can be extended by two months, but the

individual must be informed within one month. You must obtain approval from the DPO before extending the deadline.

SANHS can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, SANHS can request the individual specify the information they are requesting. This can only be done with express permission from the DPO.

Once a subject access request has been made, SANHS may not change or amend any of the data that has been requested. Doing so is a criminal offence.

Data portability requests
SANHS must provide the data requested in a structured, commonly used and machine-readable format. SANHS must provide this data either to the individual who has requested it or a named other recipient.

Right to erasure

What is the right to erasure?
Individuals have a right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed.
- Where consent is withdrawn.
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed or otherwise breached data protection laws.
- To comply with a legal obligation.
- The processing relates to a child.

How SANHS deals with the right to erasure
SANHS can only refuse to comply with a right to erasure in the following circumstances:

- To exercise the right of freedom of expression and information.
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- For public health purposes in the public interest.
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes.
- The exercise or defence of legal claims.
- If personal data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the individual asks, SANHS must inform them of those recipients.

The right to object

Individuals have the right to object to their data being used on grounds relating to their particular situation. SANHS must cease processing unless:

- SANHS has legitimate grounds for processing which override the interests, rights and freedoms of the individual.
- The processing relates to the establishment, exercise or defence of legal claims.
- SANHS must always inform the individual of their right to object at the first point of communication, i.e. in the Privacy Notice. SANHS must offer a way for individuals to object online.

The right to restrict automated profiling or decision-making

SANHS may only carry out automated profiling or decision-making that has a legal or similarly significant effect on an individual in the following circumstances:

- It is necessary for the entry into or performance of a charitable object.
- Based on the individual's explicit consent.
- Otherwise authorised by law.

In these circumstances, SANHS must:

- Give individuals detailed information about the automated processing.
- Offer simple ways for them to request human intervention or challenge any decision about them.
- Carry out regular checks and user-testing to ensure systems are working as intended.

Criminal offence data

Criminal record checks
Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject. SANHS do not normally engage in activities involving unaccompanied vulnerable people, so at this point do not foresee making such checks.

Note 4

Audits and monitoring and reporting breaches

Data audits
Annual data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. SANHS should alert the board to any potential risks.

Monitoring
The DPO has overall responsibility for this policy. SANHS will keep this policy under review and amend or change it as required.

Reporting breaches
Any breach of this policy or of data protection laws must be reported as soon as practically possible. All members, volunteers and the Office Manager have an obligation to report actual or potential data protection compliance failures. This allows the Society to:

- Investigate the failure and take remedial steps if necessary.
- Maintain a register of compliance failures.
- Notify the DPO of any compliance failures that are material either in their own right or as part of a pattern of failures.

Note 5

Third parties

Using third party or sub-processors
SANHS must only appoint processors who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected. Appropriate measures will be taken to ensure the security of the processing. Nothing will be done by SANHS to infringe on GDPR.