SANHS
Data Protection Policy

Table of Contents

The trustee responsible for data protection is Christine Webster.

Adopted by SANHS Board of Trustees on 13th June 2023

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.

The general data protection regime applies to most UK businesses and organisations. It covers the UK General Data Protection Regulation (UK GDPR), tailored by the Data Protection Act 2018. This policy has been written to ensure compliance with this Act.

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 name, title, age, address, phone number, email address, subscription details and details of education and skills. Relevant information on medical conditions is also collected for SANHS volunteers. SANHS does not collect the special categories of personal data specified in the Act (See Note 1). SANHS does not collect data on any family members under the age of 18.
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.
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 UK GDPR seven key principles of data protection. SANHS will make every effort possible in everything SANHS does to comply with these principles. The 7 principles are:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability

1. Lawfulness, fairness and transparency

- SANHS must set out exactly why data is being collected.
- The reason SANHS would be collecting data would be because **consent** has been granted – this is one of 6 legitimate reasons for collecting data. There should be clear evidence that the individual has given consent for SANHS to process their personal data for a specific purpose.
- SANHS must ensure the data will only be used for lawful purposes.
- Fairness – SANHS will only handle personal data in ways that people would reasonably expect and must not use it in ways that have unjustified adverse effects on them.
- Transparency - SANHS will be clear, open and honest with people from the start about how and why their personal data will be used.

2. Purpose Limitation. A supporter's data can only be used for the purposes specified. SANHS will only use the data for any purposes that were originally set out.

3. Data Minimisation. SANHS must ensure that only the data required is collected. SANHS should collect as little data as possible, and you should only retain the data that's necessary for ongoing operations.

4. Accuracy – SANHS must take reasonable steps to ensure the accuracy of any personal data. If it's inaccurate or outdated, the Society should either work to rectify it, or else delete it.

5. Storage Limitation. SANHS will not store members and supporters' personal data for longer than necessary. Periodic reviews to identify and delete any data no longer needed should take place. SANHS Archive Retention Policy sets out the standard retention periods for different categories of information held. SANHS has an obligation to keep to these retention periods in practice, and for reviewing retention at appropriate intervals.
Personal data no longer required should be erased or anonymised. Data should only be stored offline if there is justification for holding it. (See Archive Retention Policy for further details). SANHS must be prepared to respond to subject access requests for personal data stored offline and must still comply with all the other principles and rights.

6. Integrity and Confidentiality. SANHS must take responsibility for ensuring that all supporters' personal data is secure. Appropriate security measures must be taken to protect the data against loss, damage, and unlawful access. Paperwork which includes personal details is kept in a locked drawer until these details can be added to the Society's database. Access to electronic records are protected by passwords.

7. Accountability. SANHS has a legal responsibility to comply with GDPR and should also be able to readily demonstrate that the Society is complying with regulations.

SANHS Responsibilities in relation to GDPR

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 Controller 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. There has to be appropriate security in place to prevent the personal data held being accidentally or deliberately compromised. This includes cybersecurity (the protection of networks and information systems from attack) but also physical and organisational security measures.

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; Zoom; Restrict Content Pro and WordPress.

Storing data securely

- SANHS must ensure that data can be accessed, altered, disclosed or deleted only by those authorised to do so (and that those people only act within the scope of the authority given them)
- 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.
- Data should remain accessible and usable, ie, if personal data is accidentally lost, altered or destroyed, SANHS should be able to recover it and therefore prevent any damage or distress to the individuals concerned.
- 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.
- All servers containing sensitive data must be approved and protected by security software.
- Electronic waste should be disposed of carefully and securely.
- SANHS must keep IT equipment, particularly mobile devices, secure.
- All possible technical measures must be put in place to keep data secure.
- The SANHS office must be protected by high quality doors and locks. The SHC should be protected by alarms, security lighting or CCTV.
- Access to the SANHS office should be controlled and any visitors supervised.

Cybersecurity

This is a complex technical area that is constantly evolving, with new threats and vulnerabilities always emerging. SANHS needs to assume that IT systems are always vulnerable and take steps to protect them.

When considering cybersecurity, SANHS should ensure systems are as secure as possible by looking at:

- system security – the security of our network and information systems, including those which process personal data.
- data security – the security of the data held within our systems, eg ensuring appropriate access controls are in place and that data is held securely;
- online security – eg the security of our website and any other online service or application used; and
- device security – including policies on Bring-your-own-Device (BYOD) if offered.

SANHS should remember the following:

- cybersecurity measures need to be appropriate to the size and use of our network and information systems.
- the state of technological developments should be taken into account, but also the costs of implementation.
- the level of security must be appropriate to our business practices. For example, if staff work from home, measures need to be in place to ensure that this does not compromise security.
- measures must be appropriate to the nature of the personal data held and the harm that might result from any compromise.

Rights of Individuals

Right to be Informed

When personal data is collected from an individual, SANHS must provide them with privacy information at the time this data is obtained. This requirement can be met by putting the information on the website, but individuals must be made aware of it and have easy access to it.

If this personal data is used for any new purposes, SANHS must update the privacy information and proactively bring any changes to people's attention.
It is good GDPR practice to use the same medium used to collect personal data to deliver the privacy information.

Right of Access

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. It helps individuals to understand how and why SANHS is using their data, and check the charity is doing it lawfully.

SANHS must comply with a SAR (subject access request) without undue delay and at the latest within one month of receiving the request. The time taken to respond can be extended by a further two months if the request is complex or a number of requests from the individual have been received.

Right to Erasure

Under Article 17 of the UK GDPR, individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'.
The right only applies to data held at the time the request is received. It does not apply to data that may be created in the future. The right is not absolute and only applies in certain circumstances. Individuals have the right to have their personal data erased if the personal data is no longer necessary for the purpose it was originally collected or processed for the individual withdraws their consent.

Right to restrict processing

Article 18 of the UK GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that SANHS uses their data. This is an alternative to requesting the erasure of their data.

Processes need to be in place that enable SANHS to restrict personal data if required. It is important to note that the definition of processing includes a broad range of operations including collection, structuring, dissemination and erasure of data. Therefore, methods of restriction should be used that are appropriate for the type of processing SANHS is carrying out.

The UK GDPR suggests several different methods that could be used to restrict data, such as:

- temporarily moving the data to another processing system
- making the data unavailable to users; or
- temporarily removing published data from a website.

It is particularly important that SANHS considers how to store personal data that no longer needs to be processed but the individual has requested you restrict (effectively requesting that you do not erase the data).

If an automated filing system is being used, technical measures need to ensure any further processing cannot take place and that the data cannot be changed whilst the restriction is in place. There should be a note on the system to say that the processing of this data has been restricted.

SANHS must not process the restricted data in any way **except to store it** unless:

- the individual's consent has been obtained.
- it is for the establishment, exercise or defence of legal claims.
- it is for the protection of the rights of another person (natural or legal); or
- it is for reasons of important public interest.

Right to object

Article 21 of the UK GDPR gives individuals the right to object to the processing of their personal data at any time. This effectively allows individuals to stop or prevent SANHS from processing their personal data.

An objection may be in relation to all of the personal data held about an individual or only to certain information. It may also only relate to a particular purpose you are processing the data for.

These rights include their ability to:

- Receive information on how their personal data is being used.
- Access their personal data.
- Update any incorrect or inaccurate personal data.
- Request erasure any data you have on them.
- Stop or restrict the processing of their personal data.
- Allow them to receive or transmit their data.
- Object to how SANHS may process their data.

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.

Reference

UK https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/

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

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.

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.

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.

Note 3

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.