#  GENERAL SERVICE BOARD OF ALCOHOLICS ANONYMOUS

# SOUTH AFRICA

# DATA PROTECTION POLICY

# (UPDATED SEPTEMBER 2021)

# AIMS OF THIS POLICY

The General Service Board of Alcoholics Anonymous South Africa is committed to protecting the privacy and security of its staff, Trustees and members personal information as well as customers, suppliers and service providers.

The organisation needs to keep certain information on its employees, Trustees and members to carry out its day-to-day operations, to meet its objectives and to comply with legal obligations.

The organisation is committed to ensuring any personal data will be dealt in accordance with the Protection of Personal Information Act (POPI). To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organisation, including how the data is collected and what personal information is used.

By following good practice, AASA can protect its staff, members and Trustees as well as protecting the organisation as a whole.

This policy covers employed staff, Trustees, Sub-Committee members and fellowship members.

The Chairman of the General Service Office is the Registered Information Officer for AASA.

# DEFINITIONS

In line with the Protection of Personal Information Act (POPI) principles, The General Service Board of Alcoholics Anonymous South Africa will ensure that personal data will:

* Be obtained fairly and lawfully and in a transparent way;
* Be available for review by the data subjects at any time;
* Collected only for valid purposes that are clearly explained and not used in any way that is incompatible with those purposes;
* Relevant to the purposes collected for and limited only to those purposes;
* Be accurate and kept up to date;
* Kept only as long as necessary for the purposes it was collected for;
* Kept securely.

The definition of **‘Processing’** is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes paper based personal data as well as that kept on electronic devices, such as computers and cell phones.

The POPI Act suggests eight key principles of good data governance on which best practice is based. The organisation will seek to abide by this code in relation to all the personal data it processes, i.e.

1. **Accountability:** Those responsible for personal data should ensure they comply with the conditions and measures as set out in the POPI Act at the time of processing the data.
2. **Processing Limitation:** The collection and use of personal data must be fair and lawful and in accordance with the POPI Act. Personal data should only be obtained directly from the data subject. If personal data is to be shared with a third party or used for another purpose, the data subject’s consent should be explicitly obtained.
3. **Purpose Specific:** The collection and use of personal data must be in accordance with the POPI Act regulations and used only for the purposes agreed by the data subject.
4. **Further Processing Limitation:** Should existing personal information be required for any other purpose other than what the information was originally gathered for, confirmation will be obtained from the Data Subject again and the Data Subject will be advised of the period the personal information will be required for.
5. **Information Quality:** Data Subjects should have access to their personal information at any time to validate the accuracy and reliability of the data. Where possible, the Data Subject should be able to update their own personal information records.
6. **Openness:** Data subjects have the right to know the roles and groups of people within an organisation who have access to their personal data, who has used this data and for what purposes.
7. **Security Safeguards:** Those collecting personal data have a duty of care to protect this data throughout the data life span. The personal information should be kept in such a manner as to limit unlawful access, interference, modification, unauthorised destruction and disclosure.
8. **Data Subject Participation:** Data subjects may request whether their personal information is held, as well as the correction and/or deletion of any personal information held about them. The Data Subject has the right to request corrections to be made to the personal information held as well as the right to withdraw their consent to use their personal information at any time.

# TYPE OF INFORMATION PROCESSED

The General Service Board of Alcoholics Anonymous South Africa processes the following personal information:

**All Fellowship Members’ Personal Data**

* Names
* Email addresses
* Telephone numbers

**Additional Personal Data held for Trustees and Committee Members whose Group/Area hold a bank account**

* Physical and Postal Addresses
* Copies of identification documents
* Date of birth
* CVs (Trustees only)

**Employees’ personal data**

* Names
* Email addresses
* Addresses
* Telephone numbers
* Date of birth
* Copies of identification documents
* CVs
* Bank details
* Emergency contact details

**Professional Contacts’ personal data**

* Names
* Job Titles
* Email addresses
* Addresses
* Telephone numbers

**Personal data is kept in the following forms:**

* Electronic emails / computer files / cell phone files
* Paper letters / forms / business cards / minutes / meeting reports / directories

**Groups of people within the organisation who will process personal information are:**

* Employed staff
* Trustees
* Sub-Committee members

# RESPONSIBILITIES

Under the POPI Act, overall responsibility for personal data in a voluntary organisation, rests with the governing body. In the case of the General Service Board of Alcoholics Anonymous South Africa, this is the Board of Trustees.

All employed staff and Trustees who process personal information must ensure they not only understand, but also act in line with this policy and the data protection principles.

Breach of this policy may result in disciplinary proceedings and legal action against the Board of Trustees.

# POLICY IMPLEMENTATION

To meet these responsibilities our employed staff, Trustees and Sub-Committee members will:

* Ensure any personal data is collected in a fair, lawful and transparent manner;
* Explain why the data is needed at the start of the exercise;
* Ensure that only the minimum amount of information needed, is collected and used;
* Ensure the information used is up to date and accurate;
* Review the length of time information is held;
* Ensure it is kept safely;
* Ensure the rights people have in relation to their personal data, can be exercised

We will ensure that:

* Everyone managing and handling personal information is trained to do so;
* Anyone making enquiries about handling personal information, whether a member of staff, Trustee or Sub-Committee member, knows what the process is;
* Any disclosure of personal data will be in line with our procedures;
* Queries about handling personal information will be dealt with swiftly and politely.

# TRAINING

Training regarding the POPI Act and how it is followed in this organisation will take the following forms:

* **On induction:** a copy of this policy will be issued
* **Awareness Campaign:** All staff, Trustees and Sub-Committee members will receive a copy of this policy and any updates as required. Procedures on handling personal information will be conveyed to all members of the organisation via the standard communications channels. Ongoing training will be given as necessary.

# GATHERING AND CHECKING INFORMATION

* Before personal information is collected, the requesting party will ensure that only the minimum information required to fulfil the task is requested.
* When information is gathered, the members will be informed of how the organisation intends to use their personal data.
* To ensure that any personal information kept is accurate, the members submitting the information should be made aware how they can update, change or request their data removed from our records.
* Personal sensitive information will not be used apart from the exact purpose for which permission was given.

# RETENTION PERIODS

The General Service Board of Alcoholics Anonymous South Africa will ensure that information is kept according to the following retention periods guidelines:

|  |
| --- |
| **GOVERNANCE** |
| Board minutes | Archived |
| Sub-Committee minutes | Archived |
| Annual Reports | Archived |
| Conference Reports | Archived |
| AASA Service Meeting Reports | Archived |
| Trustee details | Archived |
| Trustee applications | Successful – until rotation outUnsuccessful - deleted |
| Charity Annual Returns | Archived |
| General correspondence | Six months unless ongoing query/legal |
| **FELLOWSHIP** |
| Group records  | Archived |
| Group contacts | Archived |
| Intergroup records | Archived |
| Region records | Archived |
| AASA Service Meeting delegate records | Archived |
| 12th Step list details | Until stop using service |
| Share Recorder details | Until stop volunteering |
| Telephone volunteers | Until stop volunteering |
| Patient details for hospital volunteers | Anonymised once volunteers in contact |
| Archives | Archived |
| Correspondence (email/mail) | 1 year unless ongoing query/legal |
| Sub-Committee member details | Archived |
| Sub-Committee applications | Successful – ArchivedUnsuccessful - Deleted |
| **STAFF** |
| Contact details (+emergency contacts) | Archived |
| CVs | Successful – ArchivedUnsuccessful - Deleted |
| References | Archived |
| Appraisals | Archived |
| General correspondence | Archived |
| Contracts | Archived |
| Diary | Archived |
|  **FINANCE** |
| Bank details: Staff / Sub-Committees / Trustees / Suppliers | 7 years (legal) |
| Supplier details | Archived |
| Gift Aid | 7 years (legal) |
| Order details (mail/online) | 3 years (legal) |
| Share subscriber | 7 years (legal) |
| Regmaker subscribers | 7 years (legal) |
| Annual Financial Statements | 7 years (legal) |
| **FINANCE con’t…** |
| Contributions: Groups / Intergroups / Regions / Personal / Conventions | 7 years (legal) |
| Estate Legacies | 7 years (legal) |
| In memoriam payments | 7 years (legal) |
| **OTHER** |
| Professional contacts | Until no longer used |
| Visitors Book | Archived |

# DATA SECURITY

The organisation will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. The following measures will be taken:

**Physical Security at GSO and Area Offices**

* Premises are secured and accessed with keys.
* Alarms are installed in offices as well.
* All visitors are required to sign in.

**Data Security**

* All staff and Trustee emails are encrypted;
* All office laptops are physically secured and electronically encrypted;
* All office portable data sources are encrypted;
* Internet access for staff is through a secure service;
* Visitors access the internet through a separate service;
* Any data transmitted by the office is encrypted;
* All office computers are secured with passwords and auto lock after one minute when unattended;
* Office desktop computers are connected to a closed network;
* Backup of office data is made through a secure encrypted server;
* All office filing cabinets/cupboards containing data are locked when not in use;
* No data is to be removed from the office unless encrypted.

Any unauthorised disclosure of personal data to a third party by an employee, member or Trustee may result in disciplinary proceedings.

# PROCEDURE IN CASE OF A BREACH

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. For example, sending personal information to an unintended addressee or theft/loss of a laptop containing personal data.

In the event of a personal data breach please complete the attached form and send it to the Office Administrator at the General Service Office.

# INDIVIDUAL RIGHTS

Anyone whose personal information we process, has the right to know:

* What information we hold and process on them;
* How to gain access to this information;
* How to keep it up to date;
* What we are doing to comply with the Act.

They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong. They can also request their data be transferred to another party.

Individuals have a right under the Act to access certain personal data being kept about them on computer and certain files. Any person wishing to exercise this right should apply in writing to:

GSO Office Administrator

PO Box 11416, Randhart, 1457, South Africa

gso@aasouthafrica.org.za

We may also require proof of identity before access is granted.

Queries about handling personal information will be dealt with swiftly and politely.

We will aim to comply with requests for access to personal information as soon as possible, but will ensure it is provided within the 40 days required by the Act from receiving the written request.

# REVIEW

This policy will be reviewed yearly (or as necessary) to ensure it remains up to date and compliant with the law.

**IF YOU HAVE ANY QUESTIONS ABOUT THIS POLICY,**

**PLEASE CONTACT THE OFFICE ADMINISTRATOR AT THE GENERAL SERVICE OFFICE.**

# DECLARATION

I confirm I have read and understood the General Service Board of Alcoholics Anonymous South Africa Data Protection Policy and will act in accordance with it.

I am connected with Alcoholics Anonymous South Africa in my capacity as a:

[ ]  Member of staff

[ ]  Trustee

[ ]  Sub-Committee member

☐ Fellowship member

Signature Print name

Please return this form to:

GSO Office Administrator,

PO Box 11416, Randhart, 1457, South Africa

gso@aasouthafrica.org.za



**FORM TO COMPLETE IN CASE OF A DATA SECURITY BREACH**

