GUIDANCE ON THE GENERAL DATA PROTECTION REGULATION

On the 25th May 2018 a new piece of legislation will come into force, the General Data Protection Regulation. It has been created to ensure that everyone has control over their personal data, including who can use it, and for what purposes. This includes any information that can identify you as an individual, for example; your name, email address, telephone number or address. It also gives individuals the right to ask organisations for access to their own data, and to amend or remove their personal data from the records held.

The new law covers any organisation that collects stores or shares any sort of personal data. Anyone who processes personal data is responsible for ensuring that this information:

- Is obtained fairly and lawfully and in a transparent way
- Collected only for valid reasons that are clearly explained and not used in any way that is conflicting to these reasons
- Relevant to the reasons it is collected and limited only to those reasons
- Be accurate and kept up to date
- Kept only as long as necessary
- Kept securely

The General Service Board, along with the General Service Offices, have been working to ensure that the charity complies with the new legislation. Although the charity has no authority over the fellowship we have listed below a brief outline of the questions considered which may be helpful for Regions, Intergroups and Groups who collect, store and/or share personal data.

1. **WHAT** personal data do we have?

The office undertook a data audit to work out exactly what personal information is held and processed. This includes both physical records and records stored digitally. For example:

- Group records
- Region & Intergroup Officers' details
- General correspondence – emails & letters
- Professional contacts
- Accounts

2. **WHY** do we use this data?

The next step was to list the reasons the data is held, make sure that it is kept for valid reasons, and that we only store the minimum data for that purpose. For example:

- Group records – *to make sure our meetings list is up to date and groups can be contacted if necessary*
- Region & Intergroup Officers' details – *so that officers can be contacted and information shared*
- General correspondence – *emails & letters – to respond to queries*
- Professional contacts – *as part of the day to day running of the office and for public information purposes*
- Accounts – *to keep a record of transactions. We have to keep details of these for legal purposes*

3. **HOW** can we protect this data and keep it secure?

We then reviewed the personal data on our list and checked to see if there is anything we more we can do to protect the individual's details. For example:

- Group records – *only a first name and telephone number is printed in the Where to Find. Amendments have been made to the pink form so members are made aware of how their data is used and have to give permission for it to be made publically available.*
- Region & Intergroup Officers' details – *the Intergroup & Regional Liaison Officers' directory is only available to officers listed within it and the online version is password protected. Each individual officer must now update their own personal details. Amendments have been made to the registration form and members can choose which of their details are shown in the directory.*
- General correspondence – emails & letters – *Both employee and trustee email addresses are now encrypted. Emails and letters are deleted after one year unless the query is ongoing or they are legally required to be kept.*
- Professional contacts – *details are only kept as long as they are still in use.*
- Accounts – *all computers are password protected and lock automatically after one minute. Legally we must keep these details for seven years.*

Once we confirmed that we are not storing any more personal data than is necessary we created a Data Protection Policy. This lists all the different data we have, the reasons we keep this data and how long we should keep it for. This policy was forwarded to all staff and trustees.

Copies of the Data Protection Policy and the charity's Privacy Policy are available to view or download from the Data Protection folder in the website's document library:
https://www.alcoholics-anonymous.org.uk/Members/Document-Library
If you would like a copy of either policy by mail please contact the General Service Office.

We also suggested the following as data protection best practice:

Email & Computer Use

- When sending emails to a group it is best to use the blind carbon copy (bcc) to list their email addresses so that they are not disclosed publically
- When an email has been dealt with delete it after six months (unless it is an ongoing query)
- Make sure any confidential data is stored securely and/or password protected
- Do not share passwords with others
- Make sure any personal data you hold is relevant and accurate

Paper Records & Files

- Care must be taken that any records containing personal information e.g. the Confidential Directory are handled and maintained securely
- Dispose of records securely e.g. shredding

More detailed information about the General Data Protection Regulation can be found at:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

By following good practice we can protect trustees, staff and members as well as protecting the charity as a whole.