WSO ADMIN

Data Security Policy

Reference: wsosecdoc002

Version: 2 Draft

Distribution:
Matthew H

Contents

1. Mission Statement

(To be agreed and ratified by the inter groups)

The main purpose of the office is to maintain and improve Alcoholics Anonymous' ability to carry the message of recovery to those affected by alcoholism. In order to achieve this it is essential that all we focus our attention on promoting Unity, Service and Recovery within the fellowship.

Our strategy to achieve this is:

1 Ensure that each inter group is represented at Office Committee meetings.

2 Centralise the storage of information for security accuracy and validity purposes in order to ensure safe and up to date information exchange within the fellowship.

3 Produce regular newsletters to inform of service initiatives and vacancies within the local service structures.

4 Encourage use of the 'mini-com' web sites, within the National Web site, as this will create greater unity.

5 The 'mini-com' web pages, which replaced the local web sites links are now available and consist of a page where local events can be highlighted.
There is also a link to local Meetings; however this link reflects the National Meeting finder, which is not always the most up-to date.

6 Encourage the flow of accurate up to date information within the fellowship to enable and empower us to best serve those in need.

2. Purpose

The purpose of this document is to provide detailed information of the 'Data Security plan' that is an integral part of the computer system used by the Western Service Office.

We need to demonstrate to Members, through discussion with Inter-Groups, the methods we employ to ensure the security and continuity of Members Personal data; in order to protect anonymity in accordance with the Traditions.

Information regarding the Data Protection Act was requested from the General Service Office, by Matthew H - ECLO; the reply he received advised us that WSO is an autonomous Group within AA, and as such, we have a moral obligation to protect Members personal details. General Service Office, being the charity main, has the legal obligation - *see appendix A*

The WSO telephone service has always had the policy that Members contact details are strictly private and are never given out by telephone Responders or Officers to anyone, for any reason. The WSO Guidelines are specific and list Private numbers separate from Public numbers that can be given out.

Tradition Nine tells us we need to organise, to some extent, to 'carry the message' So we keep it simple, but not so simple that personal anonymity prevents us from fulfilling Our Primary Purpose. Group 12 step lists, for Office and Home Responder use, need to be provided in order to put the 'still suffering Alcoholic' in touch with an appropriate 12 stepper.

Historically these lists were mainly paper copies fragmented and uncontrolled. The same data was repeated on many different lists with little or no validation. The source of this data was a mishmash of formats stored on personal computers. Aside from the obvious problems of these lists going out of date; the personal cost of printing and posting was prohibitive. This effectively meant Home Responders 12 step lists were woefully outdated, or non-existent. There where also issues around the storage of Members personal Addresses and the disposal of out of date documents.

The Office computer centralises this data; the thinking being; the least number of sources of data the easier the data is to secure control and update. The implementation of standard practises for electronic communication security, fire walls / anti-virus software / User authority policy & a backup strategy, will ensure, as far as practically possible, the security and integrity of the data.

If we adopt this policy, which is in good faith with the Data Protection Act, then we will fulfil our moral obligations.

3. Pros & Cons

At all times Members have the right to anonymity, and can request that no personal information about them be kept, electronically or otherwise.

Pros & Cons around the Implementation of the PC in the Phone Office

The benefits from cost saving and improved service have outweighed the initial and on-going running costs.

We need a robust security strategy to protect from data breach, which needs constant monitoring to keep up with the latest security trends.

We no longer pay a printing company to run off literature pack items for us.

We no longer pay expenses to Officers for printing / posting 12 step lists on their own computers.

Essential documents are always available and up to date.

Stored & backed up on a private server, all the important information is easier to manage and secure.

We no longer have the arduous task of retrieving and shredding out of date paper copies, which historically was left un-resolved, as it seemed easier to allow it to build up in boxes at the Office, generally on the pretext that it may need to be archived.

We did undertake the task of disposing of these old documents securely, (we burnt out a shredder in the process) however this didn't include any old copies that Home Responders had, the fate of those documents is uncertain.

PC awareness training required.

Human error - Revealing Members details by mistake, of course this can happen with or without an Office pc – training at the sponsoring in stage has been beefed up, but needs to be retrospectively passed onto existing responders.

4. Members Details

There is a minimum amount of information that we need to store, in order to verify Membership of AA and their involvement in Service, the minimum being:

- Member Name
- Contact Number
- Gender
- Post Code (first part)
- Email Address
- Home Group

Optional Data:
Surname / Service Role / Service rotation date

Computer Generated Reports:

- Twelfth Step Lists
- Telephone Responders (pink card holders)
- Telephone Home Responders
- Telephone Sponsors
- Telephone Trainees
- Telephone Panellers
- Telephone Crisis List
- Office Rota's
- Regional & Local Help Line Directory
- Inter-Group, Region & Sub Committee Service Officers.
- Email distribution list

These lists are available on the computer and printed for Office use.
And are also available to authorised Members via a Private Server.

Home Responders are given a link to view appropriate files on the server.

All Printed lists are clearly marked as 'Private Members information' to remind Responders not to give out Personal information.

5. Office Equipment

A Desktop PC keyboard & monitor

Operating System - Win 7 pro

Broadband service provider - Plus-net

Hp Mono Laser Printer (re-furbished)

NAS server (future)

The following items are open source (free) software

Open Office

PDF Creator

AVG antivirus software

MySql Database

External Services

Dropbox: Cloud server that will be used as a backup. Not essential once NAS is established.

NAS: Network attached storage, a server attached to our Office Modem that allows secure remote access to the essential files. Used by Officers to view and upload files and by home Responders to View 12 Step documents.
Access is via a plug-in available for PC/ Mac/ Android & Apple.

Citrix: A remote connection available through a web based interface.
This is for remote administration access to the Office PC.
To be removed when NAS is confirmed, it has a cost, which is currently funded by the user.

6. Risk Assessment

The following risk assessment chart is open to interpretation based on experience; in this case, personal experience during the four years the PC has been in operation at the Office.

Email SSL encrypts the transmission of data, not the source document or attachment; to encrypt these attachments you need a program such as 'lock lizard' which has a one time licence of $2495 which is out of our reach. Password protection of PDF files was used, but dropped as this too requires Acrobat Pro X1 costing £160 – most economic option is not to send any documents containing Members data via email instead using the file store on the server. Files are sent directly from the PC with download and viewing achieved via private key protected cloud access.

Likelihood	Score	Consequence	Score
High	6	Severe	7
Medium	4	Medium	5
Low	2	Low	3

Multiply the two appropriate scores and apply to the Pre Score in the grid below – devise measures to improve risk and re-evaluate with Post Score. If you can reduce the score by any significant reduction it will have demonstrated your commitment to the process.

Calculate +Score and recommend any action to further reduce the risk.

7. Assessment Grid

Task	Risk	Pre Score	Measures Taken	Post Score	Further Action
Operation of Office PC Access information to help callers - Sending information to Callers via Email	PC crash - loss of data - Virus infection - Inappropriate information sent out by email	4 x 7 28	Training of users - anti virus scan of incoming documents restricts the download & printing of Members information.	4 x 5 20	+8 Consider full version of anti virus – better firewall protection
Inappropriate scam/spam programs installed by users - wrong use of internet privileges	Disclosure network IP - spam emails received - heightened risk of hacking of our server	6 x 7 42	Training of users - anti virus scan - firewall - Internet access filters - User account restrictions	2 x 5 10	+32 None
Inappropriate disposal of printed documents - distribution of printed documents	Shredding may not be done correctly remote documents (home use) are at a greater risk of inappropriate disposal	6 x 7 42	Training - Administration responsible for over seeing disposal - improve control over posted out documents by not using printed copies where ever possible.	4 x 4 16	+26 None
Data Loss - equipment failure - Catastrophic event at the Office (fire burglary deliberate vandalism)	inability to provide efficient service until restoration - ability to secure systems	4 x 5 20	Backup of all important Data - Ensure Responders have the suggested sobriety periods – Training.	2 x 5 10	+10 None
Distribution of unsecure Members information using email with attachments	Unsecured email may be read or intercepted by hackers – downloads onto memory sticks may get lost or stolen	6 x 7 42	Send links to appropriate Members so they can access files from our private server. View only is the best option but involves learning to read off the screen.	4 x 5 20	+22 Implement a strict access controls, strong passwords, file access methods
Assessment Outcome >	Totals >	174	After Assessment >	76	Review Annually

8. Interpretation of the Data Protection Act

-------- Original Message --------
Subject:RE: Data Protection Act
Date: Wed, 20 Jun 2012 16:16:52 +0100
From:
To:

Hi Matthew

Below is the text of the letter you requested
(name and address removed - confidentiality).

Regarding our telephone conversation of yesterday and the information sent to you by Angela Varley the following may suggest to you a way forward on the issue of the Where to Find and anonymity.

Experience shows that any concerns are always best discussed at group conscience, and it has been useful for Inter groups to address matters of concern by opening up workshops on the subject.

As we discussed yesterday, newer members need to know that when they give their details to a Liaison Officer for the Where to Find, these details will be used for AA purposes and will be printed in either local or national meeting lists. Liaison Officers of course will need to keep lists of these contacts. If the Inter group decides to give these details to other AA entities then this should first be discussed at Inter group and agreed.

Any Where to Find is an internal publication, not intended for outside use, and it is up to members to respect this. You will note that we do not sell the national Where to Find to anyone who is not a member. Full names are not used in Where to Find and so anonymity is protected.

The Data Protection information already sent to you can be useful as a background but as we discussed yesterday, only the charity - the General Service Board - is bound by the law. The General Service Office keeps full details of those in service and we undertake to do so within the law as determined by the Data Protection Act. Groups, Inter groups and Regions are autonomous as you know and have a moral duty rather than a legal one to protect members. This protection is given to all who come to AA through the Traditions.

I hope that this has covered the points we discussed yesterday and it would be appreciated if you could let us know of any outcome of discussions at Inter group - this could be added to our bank of experience here at GSO.

We send AA love and best wishes to you and all at Somerset Inter group.

Yours in fellowship

----- Original Message -----
From: "Matthew
To: <gso@alcoholics-anonymous.org.uk>
Sent: Sunday, June 10, 2012 8:04 PM
Subject: Data Protection Act

> Hi
>
> Some time ago a friend of mine, wrote to York about the
> legality of storing peoples names and phone numbers at the Bristol
> office and on the computer. As I remember, you wrote back to us telling
> us that although we had a moral responsibility to keep members details
> confidential there was no legal responsibility because groups and
> service offices were not legal entities in them selves and only York as
> a charity was a legal entity and is subject to the data protection act.
>
>
> I wonder if you had a copy of the letter you sent to Tony or could you
> send me a similar official explanation and we can store the letter in
> the office and our guidelines to clear up any future potential
> controversy.
>
> In Bristol we are developing how we store information about our service
> structure and wish to ensure, that when asked questions from members
> about storing information, we have the official view of AA and not just
> our own opinions.
>
>
> Kind regards

9. Database User Level Security

One-step Security Wizard Report

This report contains the information you need to re-create your workgroup file and regain access to your security-enhanced database in case of corruption. It is highly recommended that you print or export this report and keep it somewhere confidential.

Unsecured Database:

C:\AA-Data\Shared Documents\Office Database\SecureOffice_be.bak

Security-Enhanced Database:

C:\AA-Data\Shared Documents\Office Database\SecureOffice_be.mdb

Workgroup Information File:

C:\AA-Data\Shared Documents\Office Database\WSO secure.mdw

User Name:

wso office

Company:

Western Service Office

Workgroup ID:

53ren1ty20%

Security-Enhanced Objects:

Tables:

dbo_South Midlands
dbo_tbl_Date
tbl_AA-Members
tbl_ArchivedRotaData
tbl_AreaCodes
tbl_AreaCodesNew
tbl_Criteria
tbl_Dap12
tbl_Days
tbl_DistibrutionList
tbl_GroupMembers
tbl_Gsr
tbl_InternationalMobileNumbers
tbl_LocalHelplineNumbers
tbl_Meetings
tbl_Months
tbl_RotaData
tbl_RotaDataHome
tbl_RotaTemplateAllShifts
tbl_RotaTemplateDayShifts
tbl_RotaTemplateHome
tbl_ServiceGroups
tbl_ShiftTimes
tbl_Statistics
xtbl_GroupMembers
<New Tables/Queries>

Queries:

qry_ResponderStats
<New Tables/Queries>

Forms:

<New Forms>

Reports:

<New Reports>

Macros:

<New Macros>

Database:

VBE Password not set

One-step Security Wizard Report 10 August 2013

10. User Level Policy

Computer:

Admin: Full access as set by Windows User Accounts

Users: Restricted access as set by Windows User Accounts

Each User Group has their own password to log on to Windows desktop

Database:

Admin: Access as set by database security wizard

User: View / Add / Edit / Print

Read Only: View / Print

Documents on Cloud Server:

Admin: Full access

Collaborator: View / Add / Edit / Upload / Download

Share: View