Family Groups Ltd

Data Protection Policy

The Al-Anon Family Groups are a fellowship of relatives and friends of alcoholics who share their experience, strength and hope in order to solve their common problems. The Al-Anon programme of recovery is based on the principle of anonymity and every effort is made to ensure that we keep data about our members to an absolute minimum.

If we need to store data about an individual, it is kept securely and accessed only by those who have a specific need for its use. When confidential data is no longer needed it is destroyed. We have added a "GDPR Compliant" clause to all contracts.

Specifically, we comply with the eight principles of Data Protection as follows:

1. Data is processed fairly and lawfully

- The organisation complies with its duties under the relevant Data Protection legislation.
- We are registered Data Controllers.
- Staff and volunteers will be trained to understand and comply with Data Protection**.**

2. Data is obtained and processed for a specific purpose

- Full names and addresses for staff are held on file for specific legal and administrative purposes e.g. employment and payroll.
- The personal details of current Trustees of the Charity are held to comply with legal requirements.
- Where members 'Gift Aid' donations we are required by HMRC to record their details.
- Where members volunteer to be a telephone contact for a group, we hold first names and telephone numbers only.
- We hold the Current Mailing Address (CMA) for the purposes of mailing the Group information and the annual record check form. It is held in confidence, is not provided to third parties or used for any other purpose.
- We hold full contact details of Helpline volunteers for the purpose of keeping them informed of changes to the index of Groups, changes to the rota and to update on training and procedures. These are deleted once the volunteer resigns from the role.
- We do not keep the names, addresses, email addresses or telephone numbers of people who call the helpline.
- We do not record helpline conversations.
- We do not save distress emails for longer than two months
- When requested to do so we take names and addresses to send literature, or reply to emails. Once answered these details are destroyed or deleted.

- We hold neither bank nor credit card details for members who donate or purchase literature.

3. We hold no more data than is necessary

- We request personal data only when it is required for a specific reason.
- We have no database of members.

4. We keep our data up to date

- Group mailing addresses are checked annually for insurance purposes via the Annual Record Check form. By completing this form, groups consent to the General Service Office using a specific name and address.
- If the ARC is not returned, the contact details are removed.
- If a volunteer asks to be removed from a service position their contact details are erased.

5. Data retention – we only keep data as long as it is needed

- Financial records are kept for seven years as recommended by HMRC.
- Once a member has completed their term of office, their details are deleted.
- Contact details for inactive groups are erased.

6. The rights of the individual are observed

- Any member may request that we delete their personal information from our records, unless we are required by law to keep it.
- Permissions once given may be withdrawn at anytime e.g. podcasts. video or shares for *Al-Anon Today* which may be used on the website and in social media.

7. Data is kept secure

- Staff and volunteers receive training during their induction period and periodically throughout their employment. All volunteers sign a confidentiality agreement.
- Confidential details held on computer are password protected.

8. Processing outside the EU

- Family Groups Ltd do not operate outside the EU.

This Data Protection Policy has been circulated to all staff and volunteers and will be reviewed annually by the General Secretary.

National Cyber Security Centre

Password security

Attackers use a variety of techniques to discover passwords, including using powerful tools freely available on the internet. The following advice makes password security easier for your users – improving your system security as a result.

How passwords are cracked...

Interception

Passwords can be intercepted as they are transmitted over a network.

Brute Force

Automated guessing of billions of passwords until the correct one is found.

Searching

IT infrastructure can be searched for electronically stored password information.

Stealing Passwords

Insecurely stored passwords can be stolen – this includes handwritten passwords hidden close to a device.

Manual Guessing

Personal information, such as name and date of birth can be used to guess common passwords.

Shoulder Surfing

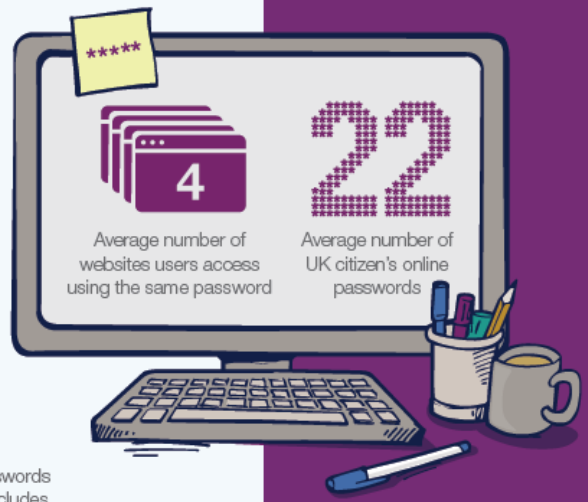
Observing someone typing their password.

Social Engineering

Attackers use social engineering techniques to trick people into revealing passwords.

Key Logging

An installed keylogger intercepts passwords as they are typed.



...and how to improve your system security

Help users cope with 'password overload'

- Only use passwords where they are really needed.
- Use technical solutions to reduce the burden on users.
- Allow users to securely record and store their passwords.
- Only ask users to change their passwords on indication of suspicion of compromise.
- Allow users to reset password easily, quickly and cheaply.

Help users generate appropriate passwords

- Put technical defences in place so that simpler passwords can be used.
- Steer users away from predictable passwords – and ban the most common.
- Encourage users to never re-use passwords between work and home.
- Train staff to help them avoid creating passwords that are easy to guess.
- Be aware of the limitations of password strength meters.

Blacklist the most common password choices

Monitor failed login attempts… train users to report suspicious activity

Prioritise administrator and remote user accounts

Don't store passwords in plain text format.

Change all default vendor supplied passwords before devices or software are deployed

Use account lockout, throttling or monitoring to help prevent brute force attacks

For more information go to www.ncsc.gov.uk @ncsc