GDPR Guidelines for Group Leaders

DATA PROTECTION GUIDELINES.

The new General Data Protection Regulation (GDPR) means that the K2 Committee should offer you some guidelines about the way in which you handle the members' personal details. In the list below, there are a number of points that you may want to consider in administering your Group.

You will almost certainly have been following the principles behind the guidelines but probably without realising it, so it is very unlikely that they will make any significant difference to the way in which your Group is run. The list is not meant to be all inclusive as all Groups are different, consequently not all of them will be applicable to how your Group is administered.

- If the membership list is computerised, use password protection on the file. With Microsoft Excel and Word, you can protect your file as follows:- Click **File > Info > Protect Workbook/Document > Encrypt with Password** then enter the password e.g. "SpelthorneK2@TW153JY". Passwords should be a combination of upper and lower case letters, numbers and other characters.
- Also it might be worth considering advising/reminding your members that their details are held on a computer.
- Limit the number of people who have access to the complete list of personal details; unless the way in which your Group works is based on members sharing their details.
- If you e-mail your members, send the messages on a "bcc" basis; however, if e-mail addresses are shared e.g. for car sharing, it is suggested that new members are made aware of this when they join your Group.
- If you print out meeting attendance lists, consider not including all personal details.
- If you organise a visit that requires a member's details to be passed to a third party, advise members of this on the application form.
- If someone leaves your Group, you should delete/destroy any records of their personal details i.e. e-mail address, postal address etc.
- If you think there may have been a "data breach" e.g. your computer has been hacked or stolen, please advise the members of your Group so that they have the option to take action to protect themselves. Please also advise the K2 Chairman and Data Protection Officer.
- If you have any questions, please contact the K2 Data Protection Officer (via the website Contacts page).