Registration with the ICO
(Appendix F to the Data Protection Policy)

The Data Protection Act 1998 and its successor legislation (the "Act") requires Data Controllers to notify (or register with) the ICO. The process of registration is a simple one, completed on-line with an annual fee.

There is an express exemption from notification for 'not for profit' volunteer groups, with the option of choosing to register voluntarily.

Read Easy groups need to be aware that exemption requires data only to be stored for the purposes of maintaining support and administrating activities for 'people who are members of the organisation or who have contact with it'. This leaves a question around data stored regarding group sponsors and donors. The phrase 'for the purpose of maintaining support of the organisation' could cover donors who have agreed to their data being held, but it is nonetheless unclear. For example, would a person who made a 'one off' gift consider it necessary for their personal data to be held to maintain support of the organisation had they made no indication of intention to support in the future?

Secondly, a key requirement of this exemption is that information is only processed "where it is necessary to administer activities for people who are members of the organisation" (namely the Management Team) or those "who have regular contact with it" (namely readers and coaches). Importantly this means ensuring data is not kept longer than is necessary, or shared with others, be that accidentally (cc'd in an email for example,) or indeed intentionally.

Therefore, there is a risk for individual Management Team Members (who by membership of the Management Team are responsible for its data), that others may not follow the group's Data Protection Policy and that this could inadvertently lead to a breach of the Act by (innocent) Members. This could mean that the group (acting through its Management Team) would thereby be in breach of the notification requirements of registration with the ICO for processing data outside of the exemption parameters as well.

A further concern is that it is a condition of the Read Easy UK Public Liability Insurance Policy, so far as data protection insurance is concerned, that groups are registered in accordance with the Act. So, a choice by a group not to register with the ICO based on the somewhat opaque exemption requirements as detailed above, could potentially lead to a breach of this Data Protection Policy (and thereby the Act), which if challenged could also bring the validity of the insurance into question.

The cautious approach is therefore for each Read Easy group to voluntarily register with the ICO. By doing so, each member of the Management Team is protected by the insurance policy if another Team member or other volunteer does not follow the Data Protection Policy and this leads to a claim for damages for breach of privacy laws against the group.

Finally, it needs to be pointed out that, while claims for damages for breach of privacy are covered by the Ansvar policy, fines incurred from the ICO for noncompliance (highly unlikely we are informed) are not covered by the insurance policy and would remain the responsibility of the local group.

Registering with the ICO

It should take about 15 minutes to complete the registration form. You will need to fill in this form in one session, so we suggest you get everything you will need to complete it before you start. You will need:

- your credit/debit card or other payment details
- details about the organisation(s) you are registering, eg, name and address of person responsible for data protection for your group
- an understanding about the types of data you process

You will also need to be able to answer the answers to the following questions:

- Someone in my place of work is responsible for making sure we comply with the Data Protection Act
- Relevant people in my place of work have been trained in how to handle personal information
- When collecting personal information, we tell people how we will use it
- We have a process in place so we can respond to requests for the personal information we hold
- We keep records of people's personal information up to date and don't keep it longer than necessary
- We have measures in place to keep the personal data we hold safe and secure