Keeping Data Secure
(Appendix D to the Data Protection Policy)

Read Easy UK and its Affiliated Groups have certain responsibilities as controllers of the personal data in our possession. Whilst this data is in our care, we must comply with the eight principles of the Data Protection Act 1998 and the Privacy & Electronic Communications (EC Directive) Regulations 2003 and their successor legislation (the "Act" and the "Regulations").

As individuals, we rightly have concerns over the security of the personal data that other individuals and organisations may have about us. Personal data is at risk of disclosure if the proper procedures are not in place, and unauthorised disclosure of personal information could have serious consequences for individuals whose data is disclosed. If such unauthorised disclosure happens within Read Easy, it could lead to a serious loss of confidence in our organisation. It may also lead to enforcement action by the Information Commissioners Office against Read Easy UK, its local affiliated Read Easy groups or against individuals.

When supplying data about any individual, Read Easy will at the same time provide guidelines on the uses to which this data may be put. We ask all who work within Read Easy, whether as volunteers or employees, to agree to these guidelines and to the security policy detailed in this document.

Background

Personal data is described in the Act as: 'Data that relates to a living individual who can be identified':

a) from that data, or

b) from that data and other information which is in the possession of, or is likely to come into the possession of the organisation

This includes data held on a computer or removable device and data held in manual form such as card indexes or printed lists of the contact details of individuals. It also includes business data if there is a named contact.

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data in accordance with the Act.

Security of personal data in your care

The following guidelines are intended to help all employees and volunteers with Read Easy to ensure the security of the personal data that may be disclosed to you by the organisation, whilst it remains in your possession.

Information you store on your computer

1) If you store personal data on a computer at home or at your office, the files must be password protected to prevent unauthorised access, as must any removable media such as laptops, memory sticks, CDs or other portable devices.

2) Personal data must not be displayed on computer screens where the information may be overlooked in your absence.

3) Laptops, memory sticks, CDs or other portable hardware that may contain the organisation's data must not be left unattended in public places or in motor vehicles even if locked in the boot and even if the hardware belongs to you personally.

4) If computers that contain the organisation's data are to be disposed of, personal data must be deleted before disposal.

Personal data held manually

1) Unauthorised access to manual files such as card indexes, or printed lists containing personal contact details, must be prevented by locking away such materials rather than leaving files on desks or tables.

2) If paper on which data is recorded needs to be disposed of, the papers must be disposed of manually; the best way to do this is to shred it.

Sharing of personal data

1) The data must not be released to any other party without the permission of the Data Protection Champion.

2) Personal details should not be given out to anyone who enquires about another's contact details, without first asking that person for their specific written permission that they are willing to be contacted by the enquirer.

3) Lists of attendees at events may include an individual's name, job title, if relevant, and company name but should not include postal addresses, email addresses or telephone/mobile numbers.

Always use 'bcc'...

Remember when sending group emails, always to use the **'bcc'** option (**'blind carbon copy')** to prevent recipients from seeing each other's email addresses. The only exception to this would be when people have given specific permission for their contact details to be used otherwise. For instance, your Management Team will probably agree for their email addresses to be shared openly with other members, so that they can contact each other freely, but you should check this with each one and would be wise to minute it.

You may also find that some Reading Coaches would like to be able to communicate with each other by email. If this is requested, you should provide a sign-up list – at a Coach Meeting or training day, for instance – which lays out at the top what you are proposing and provides space underneath for those who would like to participate to provide their email address and sign agreement for it to be shared. You can then send out an email to all those who have signed which shares their addresses openly.

When volunteering with Read Easy finishes

When you stop volunteering for Read Easy you will be asked to hand over certain records that you hold and confirm that otherwise all personal data, disclosed to you as part of your role, has been disposed of securely.

For more details, please see the full **Read Easy Data Protection Policy**, available from your Data Protection Champion or on the Read Easy website.