learn to
love to
read

Data Protection Policy

Personal data is information relating to individuals which allows them to be identified. Identification can result either directly from the information in question or from that information in combination with other information. Personal data includes such information as name, email, phone number, address as well material such as photographs and video.

The processing of personal data is governed by the **General Data Protection Regulation** - the **GDPR** - and other legislation relating to personal data and rights such as the Human Rights Act 1998.

Learn to Love to Read guarantees that we will comply with our legal obligations not to collect or retain excessive amounts of data; to store personal data securely; keep personal data up to date and to destroy it safely when it is no longer needed.

Some of our personal data will relate to children under the age of 11, e.g. photographs and reports on the progress of children who are part of our programme. Photographs will only be used when permission has been given by a parent. Other information will only be shared with those who need it to perform their job effectively.

Printed personal data must be stored securely, either in the office in a locked cabinet or in clearly labelled files in staff homes. Digital personal data is mostly stored using Dropbox. Access to this Dropbox folder is password protected.

All staff mobile devices by which personal data can be accessed must be password protected – e.g. phones, laptops and ipads.

All email and mobile contact lists must be regularly checked and all personal details which there is no current legitimate justification to hold must be deleted. When we wish to communicate with individuals about aspects of our work beyond what is needed for them to carry out their specific role, consent to store and use their details will be sought.

Organisations with which we work and with which we share data will be asked to provide us with a copy of their Privacy Notice. A list will be kept of these organisations and the date when their Privacy Notice was received. We will in turn provide them with a copy of our current Privacy Notice.

Data breaches must be reported within 72 hours to the ICO if they could lead to significant risks for individuals, i.e. volume or sensitivity is high. If email or password data is breached this must be reported to the ICO within 24 hours.

Teresa Harris is the designated point of contact for Data Protection matters is also responsible for reporting any breeches that occur.

Date of approval 27/02/2018 **Date for review** 27/02/2019