GDPR Key Facts

With the Data Protection Act (DPA) being superseded by the General Data Protection Regulation (GDPR) on 25th May 2018, it is important for schools to ensure that their systems satisfy the requirements of GDPR. When GDPR comes into force, the legal basis under which Kaumaka Ltd will hold and process personal data for pupils and users of the Fitness4Fun system is that of legitimate interest.

The DfE has issued guidance to schools on GDPR, which recommends that schools ask their system suppliers six key questions about their systems, so we have answered these questions as follows:

Scope	Which personal and special category data are contained within the system?	Fitness4Fun holds the following personal and special category data: **Pupil Data** • Basic pupil details such as forename, surname, year group, class, optional username and password and a cartoon-like avatar • On-going partaking of physical activities and healthy food choices as defined by the school **User Details** • Contact details and job title of the users who use the system in schools • Username, Password, Full Name, Role and details of system usage by the user Basic pupil details, activity/healthy options data and user login details are all entered and managed by the schools.
Sharing	Does any personal data flow from the system onto anywhere else?	**Pupil Personal Data** Schools may wish to download and/or share their inputted data with other schools, LAs, MATs, etc, but we do not share this data with any 3rd party unless we are obligated to do so by the school or as a legal requirement **User Details** We do not share user contact details with any 3rd party unless we are obligated to do so by the school or as a legal requirement
Retention	What is the system's data retention policy?	**Pupil personal data** • If the data is no longer required, schools have the ability to remove a pupil and all of the associated data relating to that pupil at any time from within the system.

		• At the end of each year of their subscription, the school initiates the new school year process which moves the children up a year group, but also removes all physical activity and healthy option data from the previous year. In effect, the live activity data has a lifespan of 12 months at any one time. • A school's dormant system data will remain on our servers for no longer than 12 months after a school's subscription comes to an end. This period has been set to cover the possibility that the school may need to retrieve this data at a later date or feel that they would like to renew their subscription and carry on. • If the school no longer wishes to use our system and would like all system data to be promptly removed then this will be done on request. **User Details** • Details of Fitness4Fun users and their system usage are retained for up to 5 years for audit purposes after which these are destroyed.
Access	How would you get the information for a subject access request out of the system?	The information required to respond to a pupil subject access request is already available through various Fitness4Fun reports, which can be output in a number of electronic formats. Other forms of subject access requests can be sent in writing to dpo@kaumaka.co.uk.
Security	How does the system ensure the security of the personal data held?	• The entire Fitness4Fun system is stored in a secure dedicated hosting environment, which is located in a secure UK-based facility (Fasthosts, ISO 27001) • The entire Fitness4Fun system operates under SSL (Secure Socket Layers) and strong AES encryption techniques used for dormant data, such as data backups. • Server access controls are only used by members of the senior development team

		• Security tests are continually carried out by our senior development team and benchmarked against external bodies such as Qualys SSL Labs. • Numerous safeguards are in place to assist schools with their access of the system, eg unique usernames, strong hashed passwords, limited number of login attempts per user, different levels of access control, ability to disable logins irrespective of the validity of the entered details, etc • All relevant staff are DBS checked and have completed non-disclosure forms.
Own Readiness	Is this system supplier confident that they will be GDPR compliant by May 2018?	Yes – to the best of our knowledge we believe that we are fully compliant with our GDPR requirements.

Our new Data Sharing / Service Level Agreement document can be downloaded from the GDPR Key Facts section of our Fitness4Fun web site