Children's Privacy Policy

Introduction

This document sets out the basis upon which we gather, store and process children's personal information where it differs from handling of adult data. The main LED Privacy Policy can be found on our website at www.ledleisure.co.uk.

.Under UK data protection law and the European General Data Protection Regulation (GDPR), we are required to tell you how we collect and use ("process") personal information.

We are entitled to process your personal information if:

a. We have a "*justification*" for doing so; or
b. We have *"consent"*.

Consents

For the purpose of this policy, LED view under 16 year olds as children. In circumstances where we believe that we may need consent to process personal data, we shall ask for a parent or guardian to confirm consent using a "*consent form.*" We shall do this separately and not bundled together with other documents. If consent is given, it may be withdrawn at a later date.

Applications for Under 16's memberships require written parental consent.

The data we collect about children

Personal data, or personal information, means any information about an individual from which that person can be identified.

We may collect, use, store and transfer different kinds of personal data about you which we have grouped together as follows:

Identity Data includes a child's first name, last name, username or similar identifier, date of birth and gender.

Contact Data includes billing and delivery addresses, email address and telephone numbers of parent(s)/guardian(s).

Medical Data includes a child's medical conditions and permission for emergency medical treatment to be given in the event of an injury or incident

Transaction Data includes details about payments for services and other details of course or products provided to the child.

Technical Data includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices used to access LED websites.

Profile Data includes username and password, purchases or orders, interests, preferences, feedback and survey responses.

Usage Data includes information about how individuals use our website, products and services.

Marketing and Communications Data We will not market directly to under 16's or pass on their information to third parties.

We also collect, use and share **Aggregated Data** such as statistical or demographic data for a variety of purposes. Aggregated Data may be derived from personal data including that of children but is not considered personal data in law as this data does **not** directly or indirectly reveal your identity.

We do not collect the following **Special Categories of Personal Data.** This includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, and genetic and biometric data.

Failure to provide personal data or consents as required for services to children

Where we need to collect personal data by law, or during the performance of a contract and there is a failure to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into. In this case, we may have to cancel a product or service ordered but we will notify the parent or guardian if this is the case at the time.

Guidelines on dealing with Children's Data

All staff who work with children are aware of their responsibilities under GDPR.

Storage and Security

Children's data should always be stored in the most secure way possible in the circumstances including as follows:

- Only those people with a genuine business need to see the data should be allowed access and they will be DBS checked.
- Where hard copies are required, these will be kept in a secure locked cabinet or equivalent with access only provided to staff with a specific need for that data.
- Any data secured electronically will be kept on a secure server or PC with firewall protection and any additional security as required in line with generally accepted current industry standards.
- Access to online data should always be password protected, with the password being changed regularly and whenever there are staff changes.