Strength Camp UK Limited

Trading as Strength Camp Chester

Introduction

Strength Camp Chester needs to gather and use certain information about individuals.
These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.
This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law GDPR.

Here at Strength Camp Chester we take your privacy and the privacy of the information we process seriously. We will only use your personal information and the personal information you give us access to under this contract to administer your account and to provide the services you have requested from us. We will always treat your personal details with respect and never sell or share them with other organisations for marketing purposes unless it is the for advertising purposes and we have permission of the client.

This policy describes how this personal data must be collected, processed, transferred, handled and stored in order to meet the requirements of data protection law, in particular the General Data Protection Regulation (GDPR). We recognise that, not only must we comply with the principles of fair processing of personal data, we must also be able to demonstrate that we have done so. The procedures and principles set out below must be followed at all times by the Company, its employees and all those within its scope as set out below.

Why this policy exists

Requirements of the Data Protection Act (DPA) 2018 and the General Data Protection Regulation (GDPR)
The DPA 2018 and GDPR set out a number of requirements in relation to the processing of personal Data.

This data protection policy ensures Strength Camp Chester:

- Complies with data protection law (GDPR) and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

These rules apply regardless of whether data is stored electronically, on paper or on other materials.
To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.
This policy is underpinned by important principles. These say that personal data must:

.

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes

- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

Key Responsibilities

- The Director is ultimately collectively responsible for ensuring that the Company meets its legal obligations and that this Policy is followed
- The Data Protection Officer (DPO) is Mr Jack Rigby who is responsible for:

    - keeping the Staff updated about data protection responsibilities, risks and issues
    - reviewing all data protection procedures (Procedure manual is available for staff to follow)and related policies, in line with an agreed schedule
    - ensuring that all systems, services and equipment used for storing data meet acceptable security standards

Personal Data

- Strength Camp will collect personal Data from clients / employee's when joining the Gym and store in a safe place that only staff have access to.

- Information will only be shared to a third party with the clients permission

- When a client / employee leaves and the information is no longer needed it is destroyed securely using a shredder and deleted from the computer and any other device being used.

Data Storage and General Security

- Passwords should never be written down or shared between any employees, agents, contractors or other persons working on behalf of the Company, no matter what their level of seniority.
- computer equipment belonging to the Company will be sited in a secure location within the office and in a position where they cannot be viewed by members of the public
- computer terminals must not be left unattended, and should be logged off at the end of the session
- personal data personal data must never be transferred on to an employee's

personal device and we will never transfer such data onto a device owned by a contractor or agent unless they have agreed to comply fully with the letter and spirit of this Policy and with the GDPR

- should not be stored on any mobile device such as laptops, tablets and smartphones without the approval of the DPO and, where it is held, only in accordance with his or her instructions and limitations
- All manual files must be stored securely in locked cabinets.
- computer print outs containing personal information should be destroyed without delay and should never be retained for scrap paper

Access to Personal Data
In relation to accessing personal data:

- employees must never access data either on a computer or in paper form, without having authority to do so
- personal data must not be shared informally and if an employee, agent, contractor, or any other third party wants access to the data, it must be formally requested from the DPO
- personal data must be handled with care, and should not be left unattended or in view of unauthorised employees, contractors or agents whether on paper or on a screen
- Where personal data held by the Company is being used for marketing purposes, it is the responsibility of Mr Jack Rigby to ensure that appropriate consents are obtained.

Organisational Measures
The Company will take the following steps in relation to the collection, holding and processing of personal data:

- All employees, agents, contactors or other parties working on our behalf will be made fully aware of their individual responsibilities, and the responsibilities of the Company, in relation to data privacy and the GDPR and they will be provided with a copy of this Policy
- in respect of these individuals and of personal data held by the Company:
    - only those persons who need access to particular personal data in order to complete their assigned duties will be granted such access
    - all persons will be appropriately trained and supervised in handling personal data
    - all persons will be encouraged to exercise caution in discussing work related matters within the workplace
    - all employees are bound by strict duties of professional confidentiality in discussing any work related matters outside the workplace, which will be adhered to and enforced
- Our methods of collecting, holding and processing data will be regularly evaluated and reviewed and the personal data held by the Company will be reviewed periodically.
- we will keep the performance of our staff, contractors and third parties under

review and, not only will we ensure that they are required to handle personal data in accordance with the GDPR and our Policy, but we will also ensure that they are held to the same standards as our own employees both contractually and in practice

Transfer of Personal Data outside the EEA

The Company may from time to time transfer personal data outside the EEA. This will only be done if one or more of the following applies to the transfer:

- it is to a territory or sector within that territory that the European Commission has determined has an adequate level of protection for personal data**,** or appropriate safeguards as determined by the supervisory authorities
- it is made with the informed consent of the data subject
- it is necessary for the performance of a contract between the data subject and the Company, or for pre-contractual steps taken at the request of the data subject
- it is necessary for important public interest reasons, or for the conduct of legal claims, or to protect the vital interests of the data subject
- It is made from a register that under UK or EU law is intended to provide information to the public and which is open to the public or to those able to show a legitimate interest in accessing it.

- **Data Breach Notification**

All personal data breaches must be reported immediately to the DPO.

If such a breach occurs, and it is likely to result in a risk to the rights and freedoms of data subjects e.g. financial loss, breach of confidentiality, reputational damage, the DPO is required to ensure that the ICO is informed without delay and, in any event, within 72 hours of the breach.

Where the breach is likely to result in a high risk to the rights and freedoms of data subjects, the DPO also needs to ensure that the data subjects affected by the breach are informed directly and without undue delay. The following information must be provided:

- the categories and approximate numbers of data subjects affected
- the categories and approximate numbers of personal data records concerned
- the name and contact details of the Company's DPO
- the likely consequences of the breach
- Details of the measures taken, or proposed, to deal with the consequences of the breach.

All staff will receive a copy and will take effect from 25th May 2018 and is authorised by:

Jack Rigby

Director

Trading as Strength Camp Chester

Company Number 11340829

Each Strength Camp is independently owned and operated